VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

IT řešení pro inteligentní dům

IT Solution for Smart House

2010 **Bc. Zbyněk Filip**

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 7.května 2010

….....

Zbyněk Filip

Poděkování

Tímto děkuji vedoucímu své bakalářské práce, panu Ing. Marianu Mindekovi, Ph.D., nejen za cenné rady a podnětné připomínky, ale také za velmi vstřícný přístup a vedení při mé práci.

Abstrakt

V této práci se zabývám návrhem systému pro řízení inteligentního domu. Cílem je připojení jednotlivých systémů budovy k počítači a následné monitorování a regulace jejich částí. Příkladem může být sledování vytápění budovy vedoucí po následné analýze k efektivnímu nastavení klíčových prvků. Tímto způsobem lze dosáhnout lepšího využití energií a také zvýšení životní úrovně obyvatel budovy. Při návrhu systému je kladen důraz na připojení stávajících systémů budovy s minimálními zásahy do již nainstalovaných a fungujících částí. V textu je popsáno hlavní řídící zařízení, způsob připojení systému vytápění, klimatizace, osvětlení, zavlažování v interiéru i exteriéru a bezpečnostního systému spolu s bezdrátovým ovládáním prvků pro přístup do budovy v podobě zámků a elektromotorů bran či závor. V další části práce je popsána řídící aplikace spolu s nastavením serveru pro zprostředkování přístupu přes webové rozhraní.

Klíčová slova

inteligentní dům, klimatizace, systém vytápění, systém osvětlení, systém zavlažování, bezpečnostní systém, bezdrátová technologie, bluetooth, sériový port, elektromagnetický zámek, komunikační rozhraní, netbook, USB, USB-COM, převodník, PISO, posuvný registr, mikrokontrolér, 4021, PIC, 12C508A, 74HC595, RxD, TxD, uživatelské rozhraní, webová aplikace, řídící jednotka, HDD, SSD, Asus eeePC 904HD, Auraton 2005, termostat, plynový kotel, Fonderie Sime SpA, Sime Family RX 26 CE IONO, stmívač, MicroDimm 500, PIR detektor, LX48A, ventil, Jablotron, Oasis, JA-82K, JA-68, ASP.NET, .NET Framework, webový server, Apache, Mod_AspDotNet, webové rozhraní, autentizace, autorizace, webový klient, XML, RS232, midlet

Abstract

In this work I give a description of IT solution for smart house. The target is to connect typical systems of a building to a computer and to monitor and control some parts of it. For example a space heating system leading after an analysis of output data to effective reorganizing of its own configuration. The purpose is to ensure effective energy usage and to increase living standards. A special emphasis is placed on connecting to current systems instalations. In this text I describe the main control device, a way to connecct a heating system, air conditioning system, lighting system, plants watering system, security system and wireless control of access points to the building. In the next part of this work I describe the main control application with server settings for web interface accessing.

Keywords

smart house, air conditioning, heating system, lighting system, plants watering system, security system, wireless technology, bluetooth, seriál port, elektromagnetic lock, communication interface, netbook, USB, USB-COM, conversion unit, PISO, shift register, microcontroller, 4021, PIC, 12C508A, 74HC595, RxD, TxD, user interface, web application, control unit, HDD, SSD, Asus eeePC 904HD, Auraton 2005, thermostat, gas boiler, Fonderie Sime SpA, Sime Family RX 26 CE IONO, dimmer, MicroDimm 500, PIR detector, LX48A, valve, Jablotron, Oasis, JA-82K, JA-68, ASP.NET, .NET Framework, web server, Apache, Mod_AspDotNet, web interface, authentication, authorization, web client, XML, RS232, midlet

Seznam použitých zkratek a symbolů

BT	-	Bluetooth
HW	-	Hardware
PIR	-	Passive Infrared sensor
PISO	-	Parallel In – Serial Out
USB	-	Universal Serial Bus

Obsah

1 Úvod

Systém pro řízení inteligentního domu, který je předmětem této práce, vznikl ze snahy vyvinout komplexní řešení pro zvýšení životní úrovně obyvatel. Hlavní myšlenkou, ať už se jedná o domácnost či například sídlo firmy, je představa budovy jako efektivně automatizovaného celku schopného samostatných vyhodnocení jednotlivých akcí či reakcí v závislosti na aktuálních stavech vstupních prvků spolu se zohledněním přednastavených konfigurací. Tento inteligentní dům, jak je v rámci práce budova nazývána, vyžaduje minimální zásah obsluhy a je schopen vykonávat automatické procesy, kterými jsou zejména rutinní činnosti obyvatel či správce budovy. Příkladem může být osvětlení vnějších a vnitřních prostor, zavlažování rostlin či ovládání zámků ve spolupráci se zabezpečovacím systémem.

Dalším přínosem systému je monitorování provozních režimů jednotlivých částí budovy, jako jsou soustavy pro vytápění či systémy klimatizace. Výhodou nepřetržitého sledování jednotlivých vstupních a výstupních prvků těchto zařízení je možnost zpětného vyhodnocení nasbíraných dat a případné nastavení celého systému pro efektivnější využití energií.

Jedním z hlavních cílů inteligentního domu je kromě zvýšení životní úrovně obyvatel a snížení spotřeby energií stávajících systémů především splnění vysokých nároků na minimální spotřebu elektrické energie vlastního řídícího systému. Za tímto účelem jsou použita úsporná zařízení, která svým provozem výrazně nezatíží celkovou spotřebu elektrické energie budovy. Důraz je kladen také na nízké pořizovací a provozní náklady, aby bylo docíleno rychlého návratu investice. Velkou výhodou použití nízkoenergetického zařízení je také možnost dlouhodobého provozu řídícího systému ze záložních zdrojů při výpadku hlavního přívodu elektrické energie. V takovém případě je systém přepnut do nouzového režimu a obsluhovány jsou pouze základní přednstavené prvky, které zajistí zejména diagnostiku vzniklého problému a uchování důležitých informací pro pozdější analýzu.

Navržený systém není konstruován tak, aby muselo dojít ke kompletnímu přeorganizování jednotlivých částí budovy či jejich přizpůsobení již ve fázi realizace projektu stavby. Takové řešení je samozřejmě i v tomto případě nejvhodnější, avšak při návrhu systému byl kladen důraz na připojení stávajících instalací v již hotové budově. Tímto se však nevylučují jisté úpravy, které musejí být k zajištění provozu uskutečněny. Cílem je rozsah těchto úprav minimalizovat a tím zajistit instalaci systému do téměř jakékoliv budovy.

Při návrhu systému byl kladen důraz také na běžnou dostupnost zařízení. Jako základní řídící jednotka byl zvolen netbook, který splňuje potřebné nároky na kompatibilitu komunikačních portů a programového vybavení, nízkou spotřebu elektrické energie, dostatečný výpočetní výkon a v neposlední řadě přiměřené pořizovací náklady.

Komunikační rozhraní mezi řídící jednotkou a připojenými stávajícími zařízeními budovy je tvořeno je tvořeno porty USB počítače spolu s připojeným převodníkem USB-COM a posuvnými registry pro rozšíření vstupních a výstupních linek systému. Tato zařízení jsou popsána v prvních kapitolách práce.

V další části je detailní popis připojení konkrétních systémů budovy k řídící jednotce inteligentního domu. Komplexní řešení zahrnuje připojení otopného systému, klimatizačních jednotek, osvětlení budovy a exteriérů, zavlažovacího systému pro vnitřní a vnější prostory a komunikaci se zabezpečovacím systémem ve spojení s ovládáním elektronických zámků. Spolu se systémem zabezpečení je zajištěna komunikace s mobilními telefony prostřednictvím bezdrátové technologie bluetooth, která umožňuje uživatelům ovládání zámků a přístupových prvků budovy v podobě dveří, bran či závor pro vjezd automobilů.

Programové vybavení systému pro řízení inteligentního domu je složeno z operačního systému na němž je spuštěn aplikačního server. V další části práce je podrobně popsáno zabezpečení a nastavení jednotlivých částí serveru včetně instalace a základní konfigurace pro spuštění systému. Uživatelské rozhraní je vytvořeno v podobě webové aplikace, která zjišťuje interaktivní komunikaci připojeného uživatele s webovým serverem. Kapitoly týkající se uživatelského rozhraní jsou brány jako samostatná část ve smyslu uživatelské příručky. Jednotlivé části systému jsou přístupné prostřednictvím běžného webového klienta, který je spuštěn na vzdáleném počítači připojeném do sítě s korektně nakonfigurovanými přístupovými právy k síťovému rozhraní řídící jednotky systému. V části práce věnující se programovému vybavení systému jsou popsány webové stránky pro přístup k jednotlivým připojeným systémům inteligentního domu, které umožňují podrobné nastavení vstupních a výstupních prvků a konfiguraci částí systému. Dále je popsána zmíněná bezdrátová komunikace s řídící jednotkou prostřednictvím aplikace spuštěné v mobilním telefonu a následné ovládání akčních členů přístupových míst v budově.

2 Hardwarové vybavení

2.1 Řídící jednotka systému

Jako řídící jednotku celého systému jsem zvolil netbook Asus eeePC 904HD, který je svým výkonem a HW vybavením plně postačující pro dané účely. Výhodou je nízká spotřeba elektrické energie. Pro další snížení spotřeby by bylo možné využít model SSD místo HD, který obsahuje paměťovou SSD kartu místo HDD pevného disku s pohyblivými částmi. Použité zařízení obsahuje mobilní procesor řady Intel Celeron M 353 pracující na frekvenci 900, 633 nebo 500 MHz, který má sice vyšší výkon než novější Intel Atom v zařízeních eeePC, nicméně s tím souvisí také vyšší spotřeba. Pro další snížení spotřeby je tedy vhodnější model s procesorem řady Intel Atom. Nicméně Celeron M podtaktovaný na nejnižší možnou uživatelskou frekvenci 500MHz zvládá ve všech směrech obsluhovat aplikaci bez problémů, takže úspora energie může být dosažena i touto cestou. Podrobnější popis zařízení je k vyhledání v publikaci [1].

Z hlediska finančních nároků lze jako nejlevnější variantu použít Asus eeePC řady 500 či 700, který je menších rozměrů, obsahuje menší operační paměť a nižší rozlišení obrazovky. Tato varianta je podle mého názoru taktéž plně dostačující pro účely řídící jednotky inteligentního domu. Nevýhodou je menší komfort při ovládání či nastavování přímo z klávesnice zařízení a velice nízké rozlišení pracovní plochy. Vzhledem k možnosti připojení přes webové rozhraní nepovažuji tento problém za důležitý, protože veškerá nastavení aplikace lze provést z jiného PC.

Výhodou použitého zařízení v podobě plnohodnotného mobilního PC je skutečnost, že samotná baterie tohoto zařízení je využita jako záložní zdroj řídícího systému inteligentního domu a v základu není potřeba vybavit zařízení přídavným záložným zdrojem. Na druhou stranu ve spojení s výkonným záložním zdrojem je zařízení schopno díky nízké spotřebě elektrické energie zůstat v provozu i několik dní po odpojení síťového napájení. To je bezesporu vynikající vlastnost zejména z hlediska spolehlivosti a efektivnosti bezpečnostního systému.

Další možností je použít jako řídící jednotku Asus eeeBox, toto zařízení však neobsahuje displej ani baterii, takže postrádá některé výše zmíněné výhody. Z mého pohledu se rozhodně vyplatí možnost správy aplikace přímo ze zařízení v případě, že ostatní rozhraní pro přístup selžou. Vzhledem ke správě zařízení samotného je tato možnost téměř nepostradatelná. Připojovat k zařízení displej a ovládací periferie například jen z důvodu zjištění nepřístupnosti portu je pak zbytečně komplikované řešení.

Pro realizaci systému je možno samozřejmě použít jakékoliv jiné zařízení podobných parametrů, kompatibilní s platformou Microsoft Windows XP a s potřebnými porty pro připojení jednotlivých částí systému. V takovém případě je však potřeba zohlednit požadavky na efektivitu řízení inteligentního domu (spotřeba elektrické energie, cena zařízení, spolehlivost, dostupnost hardware pro opravy a údržbu, výdrž zařízení při provozu ze záložního zdroje atd.).

Vhodnou volbou je také například jednodeskový počítač EMC-LX800 velikosti 3.5“ výrobce AMD, který sám o sobě obsahuje veškeré potřebné vybavení pro obsluhu všech funkcí systému řízení inteligentního domu a tudíž lze pro realizaci toto zařízení taktéž použít. Splněny budou přitom bezpochyby nejnáročnější požadavky na spotřebu elektrické energie, výrobce udává pro tento počítač 0,9W. Nevýhodou zůstává nutnost externího zobrazovacího zařízení, klávesnice a myši, v případě správy systému přímo na zařízení. Podrobnější popis zařízení je k

vyhledání v publikaci [2].

Model ASUS Eee PC 904HD je kombinací šasi z 10“ Eee PC, přičemž obrazovka je pouze 8,9" (oproti modelu řady 1000 s obrazovkou 10“). Konkrétní kus, který byl použit pro vývoj systému pro řízení inteligentního domu disponuje následujícími parametry:

Procesor: Intel Celeron M 353 900MHz
RAM: 1GB DDR2, frekvence 667MHz
Grafická karta: Intel GMA 950
HDD: 80GB 2,5" HDD, 5400 ot./min.
LCD: 8,9" WSVGA, maximální rozlišení 1024x600 (na zabudovaném LCD)
Komunikace: Wi-Fi 802.11 b/g, 10/100 Mbps ethernet
Rozhraní: 3x USB, čtečka karet SD(HC)/MMC, VGA výstup, webkamera s rozlišením 0.3Mpix
Audio: HD Audio - zvukový kodek ALC269, vestavěné stereo reproduktory, mikrofon, 1x audio vstup, 1x audio výstup
Rozměry: 266 x 191,2 x 28,5-38 mm
Hmotnost: 1,4 kg

Výdrž přiložené baterie o kapacitě 6600mAh byla odzkoušena s výsledným časem přibližně 4 hodiny a 30 minut, přičemž frekvence procesoru byla nastavena na běžnou hodnotu 900MHz a podsvícení LCD bylo na minimální úrovni. Přesnější výsledky jsou pak předmětem dalšího měření na konkrétním systému a závisí na konfiguraci koncového zařízení spolu s četností požadavků na poskytované služby v časovém úseku nouzového režimu. Jelikož bude navíc po většinu pracovního cyklu zařízení vypnutý zabudovaný LCD displej, výsledná maximální doba provozu z baterie se bude výrazně lišit.

2.2 Připojení částí systému k řídící jednotce z hlediska hardwarového vybavení

Systém řízení inteligentního domu se skládá z několika hlavních částí, které jsou připojeny přes komunikační porty k řídící jednotce a umožňují tak aplikaci ovládat koncová zařízení nebo ze zařízení odečítat hodnoty pro zpracování systémem.

2.2.1 Komunikace prostřednictvím technologie BlueTooth

Model Asus eeePC 904HD nebyl vybaven zařízením pro komunikaci prostřednictvím technologie bluetooth, proto jsem použil externí bluetooth adaptér připojený do portu USB, konkrétně model USB Bluetooth 2.1 EDR tiny adapter firmy Digitus. Důležitým kritériem při výběru adaptéru byl dosah signálu, který je u tohoto zařízení udáván až 100 metrů ve volném prostoru. V zástavbě pak tato hodnota odpovídá přibližně 30 metrům, v závislosti na předmětech stojících v cestě mezi vysílačem a přijímačem signálu. Výhodou použitého adaptéru jsou také velmi malé rozměry. Podrobnější popis zařízení je k vyhledání v publikaci [3].

V systému pro řízení inteligentního domu je adaptér využíván ke komunikaci s mobilními telefony pro bezdrátové ovládání zámků a přístupových prvků objektu jako jsou brány či závory pro vjezd do areálu.

Výrobcem udávané parametry zařízení:

- *bluetooth specifikace V1.1, 1.2, 2.0, 2.1 + EDR*
- *rozhraní USB 1.1*
- *Class 2+, dosah až 100 m*
- *napájení z USB sběrnice*
- *komunikace se všemi standardními bluetooth zařízeními*
- *kompatibilita s Microsoft Windows Vista, Vista 64, XP, XP 64, 2000*
- *79 kanálů FHSS*
- *pracovní frekvence 2.402 – 2.480 GHz*
- *přenosová rychlost až 3Mbps*

2.2.2 Převodník USB – COM

Veškerá komunikace s externími zařízeními je prostřednictvím sériových portů COM řídící jednotky. Tyto porty mohou být fyzické nebo virtuální, v závislosti na použitém PC. Model, který byl použit v tomto případě, žádné fyzické COM porty neobsahuje, proto byl použit převodník USB 2.0 na RS232, který funguje tím způsobem, že po připojení do USB portu počítače a nainstalování ovladačů je vytvořen virtuální port COM, ke kterému lze přistupovat stejným způsobem jako k fyzickému portu COM počítače. USB převodník pak zprostředkuje přenos požadované informace po USB sběrnici do koncového zařízení, které je připojeno do konektoru COM tohoto převodníku.

Parametry převodníku

Převodník firmy i-Tec s názvem USB to serial adapter RS232 Mini umožňuje připojení zařízení k jednotlivým pinům sériového portu. Komunikace pak probíhá prostřednictvím virtuálního COM portu a je stejná jako v případě, kdy počítač obsahuje fyzický port COM. Připojení převodníku do USB portu umožní uživateli komunikaci s libovolným zařízením využívajícím rozhraní RS-232 a vybaveným standardním konektorem typu Cannon 9. Použitím většího počtu převodníků je rozšířeno sériové rozhraní počítače a tím je zajištěna komunikace s požadovaným počtem externích zařízení.

Technické parametry zařízení:

- *kompatibilní s USB 1.1 specifikací*
- *podpora sériového rozhraní RS-232*
- *podpora funkce Plug & Play*
- *přenosová rychlost 500 kb/s*

Minimální systémové požadavky:

- *IBM kompatibilní PC s procesorem Pentium 233 MHz*
- *64 MB RAM*
- *USB port*
- *Windows 98SE/ME/2K/XP nebo Mac OS 8.6 a vyšší*

K zařízení je dodáváno CD s ovladači a uživatelská příručka. Specifikace převodníku je převzata z www stránek výrobce. Podrobnější popis zařízení je k vyhledání v publikaci [4].

K řídícímu zařízení pro vykonávání funkcí systému jsou prostřednictvím převodníku připojena tato externí zařízení:

- signál bezdrátového termostatu pro spínání vytápění a klimatizace
- signál pro okamžitou aktivaci a deaktivaci kotle
- signál pro kontrolu funkce oběhového čerpadla otopného systému
- signál režimu plynového kotle a klimatizační jednotky
- signál pro kontrolu funkce pojistky komínového tahu plynového kotle
- signál pro indikaci stavu bezpečnostní pojistky v případě přehřátí kotle
- signály pro řízení osvětlení objektu
- signály pohybových čidel, čidla vlhkosti půdy, teploty vzduchu, intenzity slunečního svitu a vnitřního bezpečnostního čidla přetečení
- signál z bezpečnostního systému

- signál pro spínání vnitřních ventilů zavlažování
- signál pro spínání venkovních ventilů zavlažování
- signály pro ovládání zámků a případně dalších funkcí jako jsou například ovládací serva a motory vstupních bran objektu

2.2.3 Realizace rozšíření počtu připojitelných externích zařízení

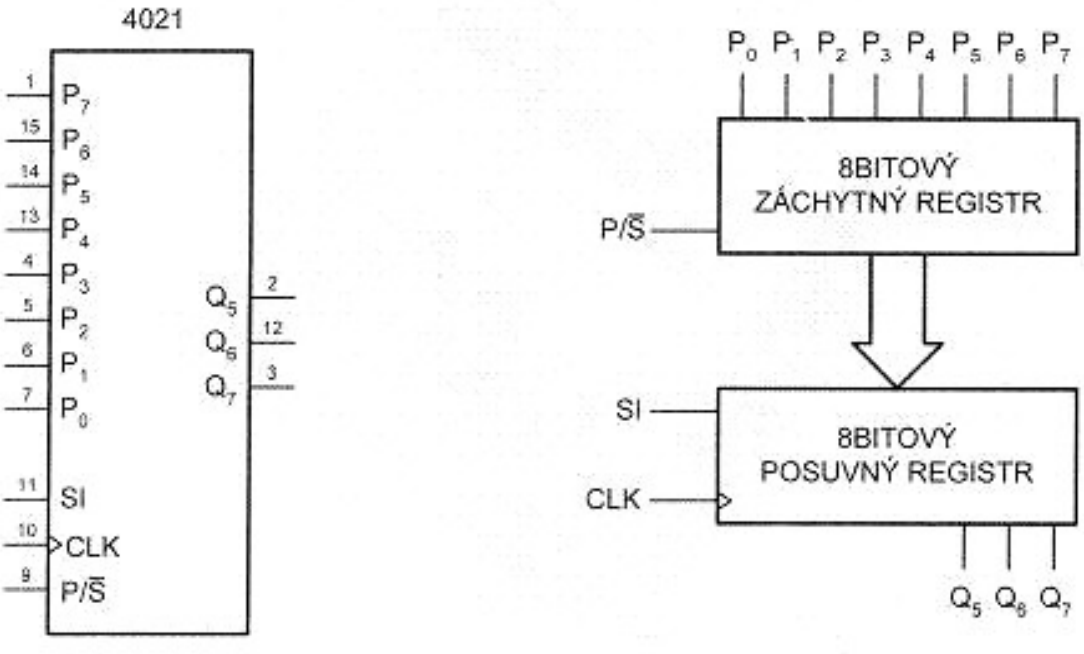
V případě systému pro řízení inteligentního domu nejsou kladeny nároky na velmi rychlé změny mezi stavy jednotlivých zařízení. Díky tomu není zapotřebí veliké množství portů tak, aby bylo nutno každý vstupní (resp. výstupní) signál vyhodnocovat (resp. ovládat) jedním konkrétním pinem příslušného portu. S výhodou lze použít posuvných registrů připojených do jediného sériového portu.

Výstupní data externích zařízení, jako jsou například čidla pohybu, jsou pak periodicky odesílána na vstup posuvného registru. Aplikace použije výstupní pin sériového portu k vyslání požadavku na odečítání hodnot ve formě logické úrovně. Tento signál aktivuje vnitřní záchytný registr připojeného posuvného registru, který zapíše do vnitřní paměti aktuální hodnoty svých vstupů. Následně odešle posuvný registr obsah vnitřní paměti po jednotlivých bitech do sériového portu počítače a tím jsou data připravena ke zpracování obslužnou aplikací.

Na podobném principu pracuje ovládání výstupních funkcí aplikace, jako je například signál pro rozsvícení světel či deaktivace zámku dveří. Aplikace pracuje s řetězcem v podobě binárního čísla, kde má každý bit příslušnost k určitému prvku externího zařízení. Tento řetězec je odeslán postupně po jednotlivých bitech z jediného pinu sériového portu na vstup dalšího posuvného registru. Potvrzování jednotlivých bitů je realizováno druhým výstupním signálem sériového portu připojeným na potvrzovací vstup posuvného registru. Počet výstupů posuvného registru je stejný jako délka zpracovávaného řetězce. Po načtení posloupnosti bitů jsou nastaveny jednotlivé výstupy posuvného registru podle hodnoty příslušného bitu v přijatém řetězci.

Druhou možností jak zajistit řízení velkého množství externích zařízení prostřednictvím velmi malého počtu dostupných pinů sériového portu je použití mikrokontroléru. V tom případě je na rozdíl od předchozího případu využit pouze jeden výstupní pin sériového portu. Tímto pinem je pin TxD pro vysílání sériových dat z komunikačního portu počítače, na rozdíl od pinů v předchozím případě, jenž byly tzv. nastavovací, tedy plnily funkci jednoduchého nastavení do jedné ze dvou logických úrovní. Přes zmíněný pin TxD jsou aplikací vyslána data v podobě hexadecimálních hodnot ukončená znakem #13 pro indikaci konce přenášené informace. Mikrokontrolér tato data přijme a nastaví výstupní obvody tvořené posuvnými registry stejným způsobem, jako v předchozím případě, kdy bylo využito pouze posuvných registrů bez asistence mikrokontroléru. Výhodou tohoto řešení je výše zmíněná úspora využitých pinů sériového portu, takže nevyužité piny mohou zůstat v záloze pro případnou obsluhu dalších zařízení u nichž může být například požadována rychlejší změna mezi jednotlivými stavy a připojení přes posuvné registry by tímto nepříznivě ovlivnilo jejich funkci.

2.2.3.1 Rozšíření vstupních linek

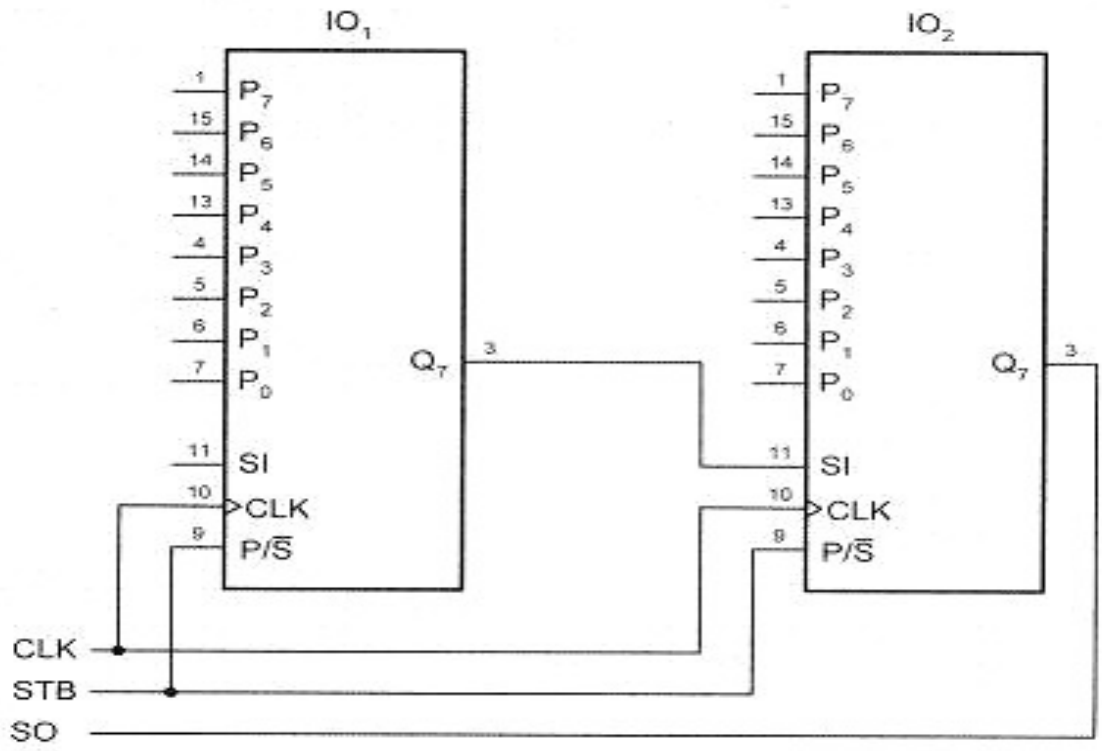


Obr.1: Posuvný registr vstupních signálů

V tomto případě je použit integrovaný obvod s označením 4021, který obsahuje posuvný registr typu *PISO*. Tento obvod umožňuje zachycení obsahu paralelních vstupů do vnitřního registru a sériové odeslání těchto dat postupně po jednotlivých bitech ze svého výstupu. Režim činnosti obvodu je nastaven vstupem P/S, který je napojen na výstupní pin DTR sériového portu počítače. Logickými úrovněmi výstupního pinu DTR lze pak ovládat jednotlivé funkce obvodu. Je-li DTR nastaven na logickou úroveň 1 (resp. High či True), tato úroveň se přenese na pin P/S posuvného registru a obvod 4021 provede načtení paralelních dat do vnitřního záchytného registru. Následným nastavením P/S prostřednictvím pinu DTR na logickou úroveň 0 (resp. Low či False) je obvod přepnut do režimu pro čtení dat ze sériového výstupu. Na výstupu Q7 obvodu 4021 je k dispozici postupný výpis jednotlivých bitů obsažených v záchytném registru. Tento výstup obvodu je napojen na vstupní pin COM portu počítače s označením CD, odkud pak příchozí hodnoty načítá aplikace a umožňuje další zpracování. Jako první bit v řadě sériových dat vysílaných posuvným registrem je obsah paralelního výstupu P7 obvodu 4021. Pro přečtení dalšího bitu v pořadí je zapotřebí potvrdit posun signálem na pin CLK obvodu 4021. Tento pin je ovládán výstupním pinem RTS portu počítače. Posun bitů na výstupu obvodu 4021 je potvrzován náběžnou hranou signálu pro pin CLK, tedy nastavením výstupu RTS portu počítače na logickou úroveň 1. Tímto postupem je umožněn průchod celým polem zaznamenaných hodnot záchytného registru obvodu 4021. Data jsou postupně z výstupu Q7 posílána na vstup sériového portu počítače, odkud jsou aplikací ukládána do vnitřní struktury programu. Následuje jejich zpracování ve formě rozkódování jednotlivých bitů a zjištění příslušnosti ke konkrétnímu externímu zařízení.

Posouváním výstupních dat obvodu 4021 náběžnou hranou signálu CLK je postupně přečtěn uložený obsah paralelních výstupů obvodu. Při odeslání náběžné hrany na pin CLK po přečtení posledního bitu sériového výstupu obvodu 4021 dojde ke čtení vstupu SI, který

umožňuje kaskádní spojování více posuvných registrů. Popsané zapojení umožňuje připojit maximálně 8 externích zařízení. Z toho důvodu je pro potřebu dalšího rozšíření použít několika posuvných registrů, které jsou vzájemně propojeny. Připojení dalších registrů je prováděno podle následujícího schématu.

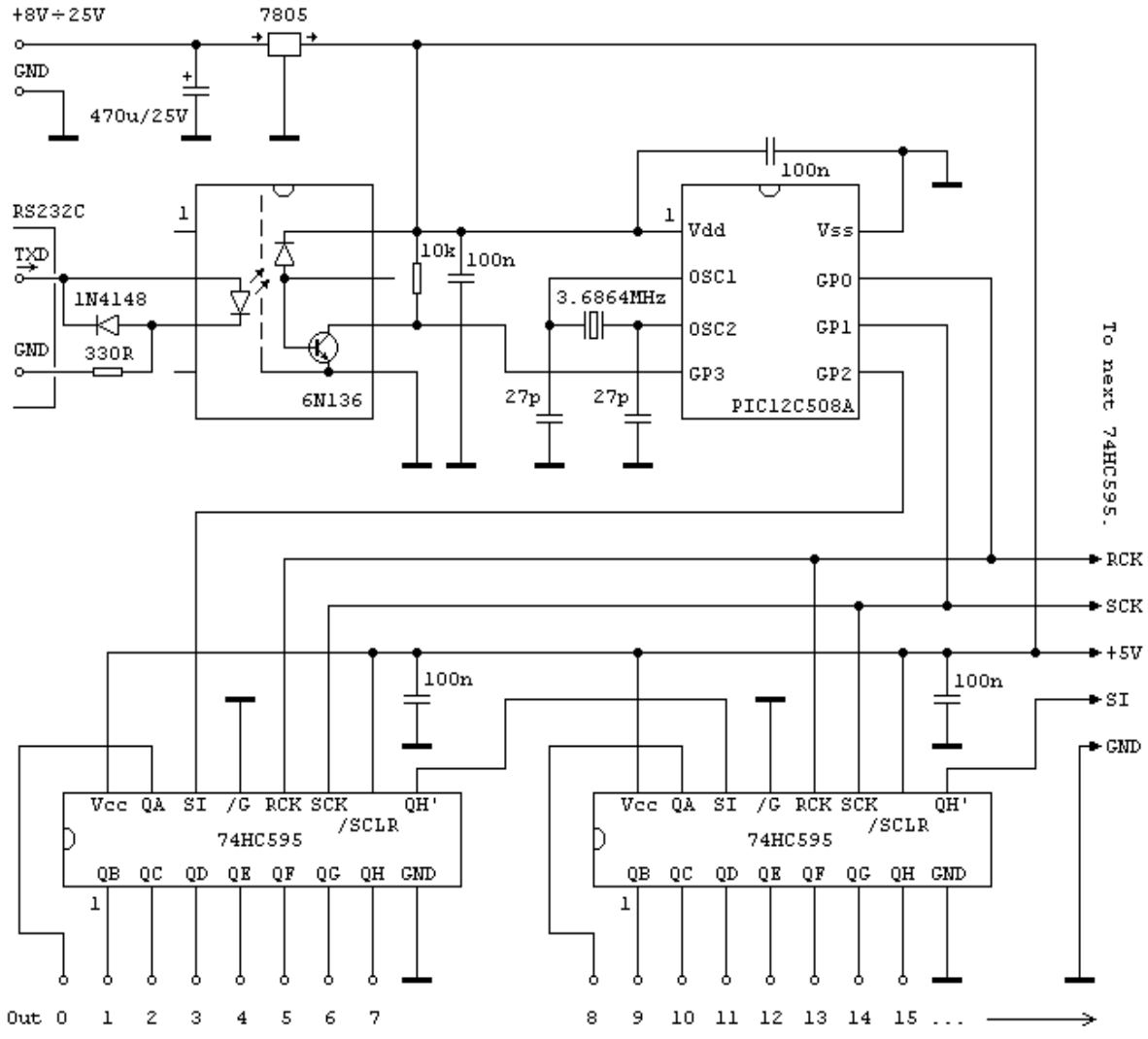


Obr.2: Rozšíření vstupních linek systému

Při posunu za poslední bit sériového výstupu posuvného registru IO2 prostřednictvím náběžné hrany signálu CLK pak dojde ke čtení dat ze vstupu SI registru IO2. Na tento vstup je připojen výstup posuvného registru IO1 a jsou tedy načítána data obsahující stav paralelních vstupů právě tohoto obvodu. Tímto spojováním posuvných registrů dohází k rozšíření počtu připojitelných externích zařízení. K popisu obvodu 4021 bylo využito publikace [5].

2.2.3.2 Rozšíření výstupních linek

Pro ovládání většího počtu zařízení připojených k počítači prostřednictvím jediného sériového portu je použit mikrokontrolér PIC 12C508A ve spojení s posuvným registrem 74HC595.
Vlastní zapojení je realizováno podle následujícího schématu.



Obr.3: Mikrokontrolér pro ovládání výstupních zařízení

Jak je již výše popsáno, ke komunikaci tímto modulem je využit jediný komunikační pin sériového portu počítače s označením TxD. Tento pin je určen k výstupu sériových dat z portu (odtud název Transmit Data). Komunikace počítače s modulem pak spočívá v

jednoduchém zápisu na sériový port, kdy je podobně jako v předchozím případě odeslán řetězec dat určujících nastavení výstupních pinů modulu, avšak tentokrát je řetězec v hexadecimálním tvaru. Ukončení řetězce je idikováno příkazem #13, který je odeslán na konci dat.

Modul mikrokontroléru převede hexadecimální číslo do binární podoby a zapíše hodnoty po jednotlivých bitech do posuvných registrů, jejichž výstupy jsou pak nastaveny podle načtených hodnot. Na vstup modulu lze odeslat v podstatě libovolně dlouhý řetězec hexadecimálních znaků, výsledný výstup pak závisí na počtu použitých registrů v modulu. Je-li řetězec po převodu na binární číslo delší než celkový počet výstupů registrů, pak dojde jednoduše k přetečení přebytečných dat. Tím budou zároveň nastaveny pouze ty paralelní výstupy, které jsou fyzicky dostupné prostřednictvím posuvných registrů. Podrobnější informace k obvodu mikrokontroléru jsou k vyhledání v publikaci [6].

2.2.4 Převod napěťových úrovní

Pro převod odlišných napěťových úrovní sériového portu počítače a posuvných registrů jsou použity jednoduché přídavné obvody. Vstupní linky posuvných registrů pro snímání dat z jednotlivých externích zařízení jsou připojeny přes napěťové děliče. Spínání výstupních akčních členů systému řízení inteligentního domu prostřednictvím jednotlivých výstupů posuvných registrů je realizováno modulem s polovodičovým prvkem nebo relé v závislosti na energetickém zatížení obvodu. Výstupní signál je přiveden na vstup modulu a podle logické úrovně je sepnut či rozepnut výstupní prvek, který je dimenzováno na potřebnou proudovou zátěž připojeného akčního členu (elektromotor, elektromagnetický ventil aj.). Vstupní zařízení generují výstupní signál s různou hodnotou napětí, podobně i výstupní akční členy musí být ovládány odpovídajícím napětím spínaným přidruženým relé. Použití vhodných převodníků napěťových úrovní je proto otázkou konkrétní konfigurace systému pro řízení inteligentního domu.

2.3 Připojení zařízení otopného systému

Systém řízení inteligentního domu umožňuje připojení stávajícího zařízení pro vytápění objektu. Prostřednictvím posuvných registrů jsou důležité prvky tohoto zařízení připojeny na vstup sériového portu počítače. Monitorování stavu a režimu vytápění lze pak využít k efektivnějšímu nastavení celého otopného systému a tím k úspoře energií a finančních investic.

Tato funkce systému má pouze informativní charakter, veškeré nastavení jednotlivých prvků otopné soustavy pro efektivnější využití energií pak probíha v rámci vlastního systému vytápění nezávisle na systému pro řízení inteligentního domu. Ten však následně umožní monitorování změněných hodnot a poskytne nové výsledky pro zvážení, zda byly úpravou vytápění splněny požadavky. K řídící jednotce jsou připojena následující zařízení.

2.3.1 Bezdrátový přijímač signálu z termostatu

K regulaci vytápění objektu lze použít například bezdrátový digitální termostat Auraton 2005, který vysílá signál pro bezdrátový přijímač umístěný v blízkosti kotle. Výstup tohoto přijímače spíná režim chodu plynového kotle. Termostat je instalován v místnosti, kde je požadována regulace teploty vzduchu. Citlivý snímač teploty v modulu termostatu dokáže zohlednit momentální podmínky v místnosti a podle toho řídit režim vytápění. Jako příklad lze uvést zapnutí televizoru a osvětlení v místnosti, což jsou nečekaně aktivované zdroje tepla.

2.3.2 Oběhové čerpadlo

Tento signál je napojen na výstup plynového kotle, který spíná čerpadlo pro oběh kapaliny v otopném systému. Význam snímání tohoto signálu je v monitorování poruchy čerpadla a také pro pozdější nastavení rychlosti otáček čerpadla pro efektivnější vytápění.

2.3.3 Snímač režimu plynového kotle

Pokud obdrží plynový kotel od bezdrátového termostatu požadavek na vytápění, pracuje v režimu vyhřívání zásobníku kapaliny a následně v režimu stand-by, kdy dochází k oběhu ohřáté kapaliny v otopném systému. Jakmile teplota kapaliny klesne pod nastavenou hodnotu, kotel začne opět zásobník s kapalinou vyhřívat. Tyto režimy se opakují až do okamžiku deaktivace kotle, například signálem od bezdrátového termostatu. Na poměr času mezi režimem vyhřívání a stand-by má vliv několik prvků a jevů, Příkladem může být počet a objem otevřených či uzavřených radiátorů v objektu, teplota kapaliny při aktivaci vyhřívání, teplota vedení otopného systému či aktuální teplota v místnostech. Sledování režimu kotle je využito pro efektivnější nastavení systému vytápění objektu a zároveň pro hlídání poruchy kotle.

2.3.4 Pojistka komínového tahu

V závislosti na technologii, kterou využívá kotel pro svou funkci, je možnost připojení různých bezpečnostních prvků kotle k sériovému portu počítače. Pojistka komínového tahu je bezpečnostní zařízení, které zajistí spolehlivé vypnutí kotle v případě negativní změny v odtahu spalin. Tato změna může být způsobena například změnou tlaku ve venkovním prostředí či ucpáním potrubí pro odtah spalin z objektu. Význam snímání této poruchy je pro signalizaci režimu vytápění. Plynový kotel je vždy umístěn mimo obývanou část budovy a deaktivace kotle na základě této poruchy má bez signálu obsluze negativní dopad na pohodlí obyvatel, jelikož změna teploty v místnosti není okamžitá. Pokud se tato porucha vyskytne například v noci, tak může dojít k výraznému snížení teploty v místnostech z důvodu neaktivního vytápění. To má za následek výrazné snížení pohodlí obyvatel. Je-li při poruše vyslán sinál obsluze, mohou být téměř okamžitě podniknuty potřebné kroky pro odstranění poruchy a obnovení vytápění budovy.

2.3.5 Pojistka přehřátí kapaliny v zásobníku

Toto bezpečnostní zařízení zajistí deaktivaci kotle při teplotě vyšší než nastavená mez (většinou hodnota 95°C), aby nedošlo k poškození či k jinému nebezpečí vlivem přehřátí zařízení. Tento signál je snímán pro okamžité upozornění na poruchu prostřednictvím řídící

jednotky inteligentního domu a může být využit pro pozdější vyhodnocení charakteru vzniklého problému, například v souvislosti s jinými naměřenými hodnotami a zaznamenanými signály v systému.

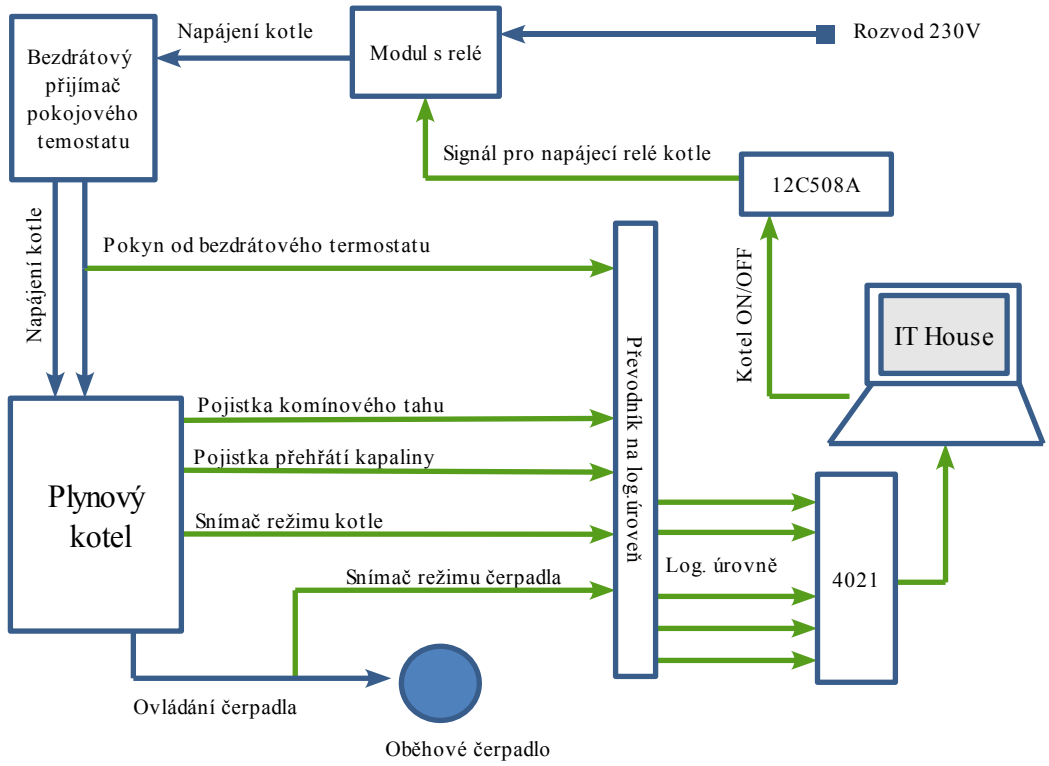
Jednotlivé signály z vytápěcího systému jsou vedeny na paralelní vstupy posuvného registru, kde každý signál tvoří jeden bit. Tento bit je pak součástí binárního řetězce, který je načten z výstupu posuvného registru do sériového portu počítače a dále zpracován aplikací. V případě bezdrátového přijímače signálu z termostatu je odečítán výstup bezdrátového přijímače v podobě dvou logických úrovní, které značí požadavek na zapnutí či vypnutí kotle. U signálu pro monitorování chodu čerpadla je snímán výstup kotle pro aktivaci a deaktivaci čerpadla v podobě jedné ze dvou logických úrovní. Snímač režimu plynového kotle a snímače stavu bezpečnostních pojistek jsou připojeny na výstup řídící jednotky kotle podle konkrétního schématu zapojení elektronické části kotle.

2.3.6 Aktivace a deaktivace kotle

Jediným výstupním členem systému řízení inteligentního domu pro připojení otopného systému je signál pro přímou dálkovou aktivaci a deaktivaci kotle. Výstupní pin posuvného registru ovládaného sériovým portem je připojen na modul obsahující relé, které je dimenzované na proudovou zátěž použitého kotle. Tento modul je použit jako mezičlánek pro napájení kotle a prostřednictvím uživatelského rozhraní jej lze nastavit do sepnutého nebo vypnutého režimu.

2.3.7 Systém vytápění rodinného domu

Funkci monitorování otopného systému jsem vyzkoušel na systému vytápění rodinného domu prostřednictvím litinového plynového kotle italské firmy Fonderie Sime SpA. Kotel nese označení Sime Family RX 26 CE IONO, jedná o verzi s elektronickým zapalováním a ionizačním hlídáním plamene. Připojení jednotlivých prvků pro snímání otopného systému řídící jednotkou inteligentního domu záleží na konkrétní stávající instalaci, zejména pak na možnostech technických úprav v podobě připojení snímačů na jednotlivé řídící a bezpečnostní prvky kotle. Výše zmíněný model poskytuje po minimálním zásahu do instalace kotle připojení všech požadovaných prvků ke vstupním posuvným registrům systému řízení inteligentního domu. Blokové schéma připojení stávající otopné soustavy je na obr.ázku 4. Propojení šipkami znázorňuje směr toku ovládacích signálů a načítaných dat. Zelenou barvou jsou vyzačeny vstupní informace systému a signál pro výstupní akční člen ovládající napájení kotle.



Obr*.4: Blokové schéma propojení otopné soustavy se systémem řízení inteligentního domu*

Připojení jednotlivých částí systému vytápění k řídící jednotce inteligentního domu je realizováno prostřednictvím posuvných registrů, které jsou napojeny na příslušné piny USB-COM převodníku.

Systém vytápění používá ke komunikaci s řídící jednotkou celkem 5 vstupních pinů posuvného registru.

Bezdrátový přijímač signálu z termostatu

Výstupní signál pro spínání kotle je přiveden na vstup modulu pro generování logické úrovně podle vstupního napětí. Při sepnutém výstupu bezdrátového přijímače je generována log 1, vypnutý výstup pak generuje log 0.

Oběhové čerpadlo

Snímání režimu čerpadla je zajištěno podobně jako v případě bezdrátového přijímače. Do napájecí cesty čerpadla je zapojen modul, který zajistí převod vstupního napětí na jednu ze dvou logických úrovní potřebných pro načtení posuvným registrem.

Připojení snímače režimu kotle

Pro snímání provozního režimu kotle jsem použil jednoduchého převodníku stavu sepnutí relé na logickou úroveň pro posuvné registry řídící jednotky. Kotel obsahuje termostat, který podle teploty kapaliny v zásobníku a potenciometru pro nastavení výkonu kotle spíná aktivní prvek vyhřívání v podobě systému hořáků. Na výstup termostatu jsem připojil snímač, který při aktivaci vyhřívání zásobníku kapaliny zajistí sepnutí polovodičového prvku a tím

poskytne informaci o provozním režimu kotle připojené řídící jednotce inteligentního domu.

Pojistka komínového tahu

Připojení snímače pojistky komínového tahu může být provedeno dvěma způsoby. Prvním z nich je napojení modulu pro načtení logické úrovně přímo k výstupu řídící jednotky, který je určen pro aktivaci pojistky. Druhou možností, která byla využita, je připojení modulu podobně jako u čerpadla, tedy přímo do elektrického vedení na vstupu do ovladače modulu pojistky v ovládacím panelu kotle. Napětí, kterým je aktivována pojistka a následně deaktivován kotel, je převedeno na logickou úroveň a pak může být dále zpracováno posuvným registrem..

Pojistka proti přehřátí kapaliny v zásobníku

Tato část kotle je připojena stejným způsobem jako pojistka komínového tahu. Modul je připojen na relé, které je součástí kotle a plní funkci deaktivace vyhřívání kapaliny při dosažení maximální přípustné teploty.

Výstup na modul s relé pro aktivaci a deaktivaci kotle

Výstupním signálem systému řízení inteligentního domu v rámci vytápění objektu je povel k okamžité deaktivaci či aktivaci kotle. Tato informace je z výstupního posuvného regitru připojeného k portu počítače odeslána do ovládacího modulu, který v případě log 1 na svém vstupu aktivuje elektromagnetický kontakt relé a tím dojde k rozpojení přívodu elektrické energie pro napájení kotle. V případě, že je na vstup modulu odeslána log 0, napájení kotle je obnoveno a dojde k opětovné aktivaci vytápění. Ovládání těchto režimů je dostupné z uživatelského rozhraní obslužné aplikace.

2.4 Připojení systému klimatizace

Systém klimatizace je k inteligentnímu domu připojen podobně jako systém vytápění výhradně z důvodu monitorování jednotlivých částí. Natavení režimu klimatizace ani vlastní regulace se neprovádí prostřednictvím systému pro řízení inteligentního domu, ten slouží pouze pro vyhodnocení průběhu klimatizačních cyklů a k analýze následných změn. Tyto změny jsou pak provedeny přímo prostřednictvím nastavovacích prvků systému klimatizace a po opětovném vyhodnocení naměřených dat systémem inteligentního domu lze určit, zda došlo k požadovaným výsledkům či nikoliv.

2.4.1 Provozní režimy klimatizace

Klimatizace mají podle výbavy jednotlivých částí možnost pracovat v režimu chlazení, odvlhčování, běžné ventilace nebo v případě osazení tepelným čerpadlem také vytápění prostoru. Teplotu vzduchu v místnosti spolu s přepínáním jednotlivých režimů je možné nastavit manuálně přímo na ovládacím panelu nebo případně dálkovým ovládáním řídící jednotky klimatizace. Pracuje-li klimatizace v režimu chlazení, pak je ve venkovní jednotce prostřednictvím kompresoru stlačováno chladivo a tím dochází ke kondenzaci. Chladivo poté prochází tepelným výměníkem , po předání tepelné energie venkovnímu prostředí pokračuje do vnitřní jednotky klimatizace, kde prochází vnitřním tepelným výměníkem v němž se začne odpařovat. Přes tento výměník je ventilátorem z vnitřních prostor nasáván teplý vzduch a po ochlazení je vháněn zpět do místnosti.

Je-li klimatizace osazena tepelným čerpadlem, umožňuje přitápění ve vnitřních prostorách obrácením procesu chlazení. Vzduch uvnitř místnosti je pak prostřednictvím klimatizace naopak ohříván.

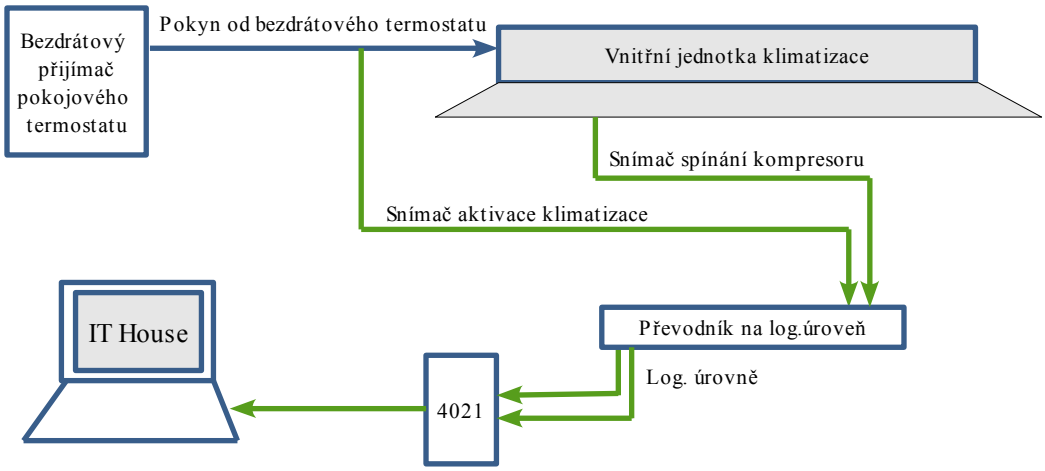
Klimatizace je složena ze dvou hlavních částí – vnější a vnitřní jednotky. Venkovní jednotka je složena z kompresoru, který zajišťuje tlak chladiva v chladícím okruhu, dále pak z tepelného výměníku a ventilátoru. Vše je spojeno potrubím a řízeno prostřednictvím ventilů. Jednotka uvnitř budovy je složena z tepelného výměníku s ventilátorem, filtrů, klapek pro nastavení směru proudění vzduchu a řídící jednotky pro ovládání klimatizace.

2.4.2 Připojení klimatizace

Pro regulaci teploty v klimatizované místnosti lze použít vnitřní teplotní snímač klimatizační jednotky a jako přídavný aktivační prvek také výše zmíněný bezdrátový termostat Auraton 2005, který byl použit při regulaci vytápění objektu. V režimu vytápění je tento termostat nastaven tak, aby v případě poklesu teploty v místnosti aktivoval vytápění a po dosažení horní přednastavené hranice teploty vytápění opět deaktivoval. Po přepnutí do režimu klimatizace pracuje regulace opačným způsobem, kdy při zvýšení teploty na přednastavenou mez dojde k aktivaci výstupního obvodu a poklesem teploty ke spodní hranici je výstup deaktivován. Výstupem je řízen bezdrátový přijímač, který spíná koncové zařízení v podobě klimatizace či v předchozím případě kotel pro vytápění. Připojení klimatizace k systému řízení inteligentního domu je znázorněno na obrázku 5.

K sériovému portu počítače je připojen výstup bezdrátového přijímače a snímač provozního režimu klimatizace. Zapojení je realizováno v závislosti na použitém zařízení klimatizace. Výstup řídící jednotky klimatizace určený pro spínání kompresoru pro cirkulaci chladícího média je připojen k převodníku na logickou úroveň, který zpracovaný signál odesílá

na vstupní pin posuvného registru. Stejným způsobem je připojen výstup bezdrátového přijímače, logická úroveň je pak přivedena na další pin posuvného registru.



Obr.5: Připojení částí klimatizace k řídícímu systému

Podobným způsobem jako kotel u systému vytápění je také napájení klimatizační jednotky připojeno přes modul s relé, který umožňuje zapnutí či vypnutí celého chladícího systému prostřednictvím uživatelského rozhraní systému pro řízení inteligentního domu. Vstup tohoto modulu je připojen na výstupní posuvný registr, který je výstupem sériového portu.

Aktuální stav vstupních pinů posuvného registru je periodicky načítán přes sériový port a zpracován aplikací. V závislosti na přednastavené konfiguraci jsou provedeny požadované akce.

2.5 Připojení systému osvětlení objektu

Řízení osvětlení objektu prostřednictvím aplikace v počítači je zajištěno kombinací přednastaveného programu pro osvětlení, výstupních signálů pohybových senzorů a samozřejmě koncových členů v podobě svítidel. Tato část je věnována způsobu připojení pohybových čidel jako vstupních zařízení sériového portu a připojení výstupních zařízení, kterými jsou svítidla.

Počet připojených pohybových senzorů a svítidel závisí na konkrétním případu realizace řízení inteligentního domu. Maximální počet připojitelných zařízení závisí na návrhu modulu pro připojení vstupních a výstupních zařízení, přesněji na rozsahu použitých posuvných registrů.

Pro připojení svítidel je využit výstupní modul s mikrokontrolérem a posuvnými registry. Jednotlivé osvětlovací prvky jsou připojeny na paralelní výstupy posuvných registrů, odkud jsou nastaveny jednotlivé režimy osvětlení. Svítidla mohou být zapojena ve dvou režimech. Prvním z nich je režim *vypnuto/zapnuto*, který spočívá v jednoduchém spínání osvětlení prostřednictvím logické úrovně příslušného posuvného registru. Druhý režim spočívá v možnosti nastavení intenzity osvětlení u svítidel vybavených stmívacím modulem. Tuto funkci lze využít například v případě nočního osvětlení výkladních skříní, bezpečnostního osvětlení venkovních prostor objektu nebo v případě nočního osvětlení obývacích prostor tak, aby nedošlo k nepříjemné reakci oka přizpůsobeného na tmu při náhlém zvýšení intenzity světla na plnou úroveň. Každé svítidlo je připojeno k jednomu výstupu posuvného registru. Přestože je výstup pouze dvoustavový, lze jím ovládat oba režimy zapojení svítidel, tedy včetně regulace intenzity světla. Přesnější princip této regulace je popsán dále v textu.

Řízení jednotlivých svítidel je prováděno prostřednictvím aplikace, která má nastavenu příslušnost bitů výstupního řetězce k jednotlivým osvětlovacím prvkům. Ke každému svítidlu je přiřazen jeden nastavovací bit. Tyto bity jsou nastaveny aplikací a celý hexadecimální řetězec obsahující bity pro výstupní externí zařízení systému je odeslán přes sériový port na vstup mikrokontroléru. Ten provede rozdělení bitů na jednotlivé výstupy posuvných registrů a tím je zajištěno nastavení aktuálního režimu osvětlení.

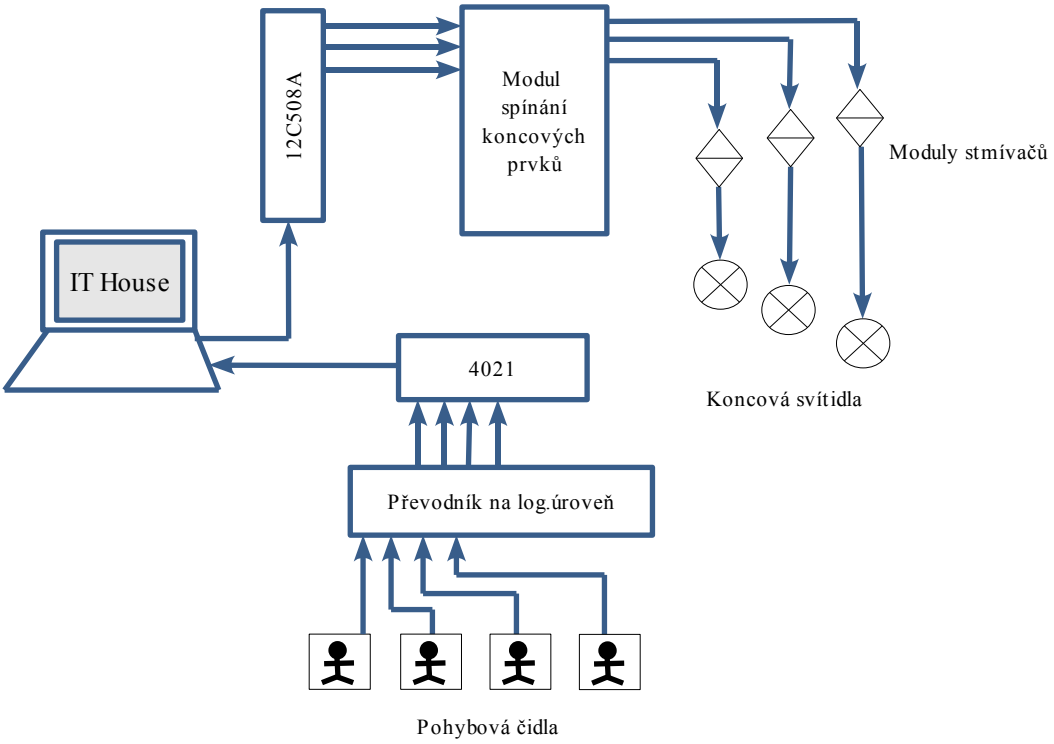
Dalšími parametry, kromě přednastaveného režimu osvětlení v závislosti na čase, jsou výstupní hodnoty pohybových čidel rozmístěných na potřebných místech vnitřních i venkovních prostor objektu. Aplikace, která zajišťuje řízení inteligentního domu, pracuje s osvětlovacím systémem ve třech režimech. V prvním režimu jsou aktuální data z pohybových čidel načtena ze sériového portu a aplikace zajistí vliv těchto dat na výsledné nastavení osvětlení. Druhý režim pracuje pouze s nastavením osvětlení v závislosti na čase a údaje z pohybových senzorů jsou v tomto případě ignorovány. Poslední režim je kombinací dvou předchozích, osvětlení je tedy ovlivněno nastavením časového intervalu a zároveň výstupní hodnotou příslušného pohybového senzoru. Mezi oběma rozhodujícími prvky platí v tomto režimu pro vyhodnocení vztah logické konjunkce. Nejsou-li tedy splněny obě podmínky, osvětlení není aktivováno. Využití této funkce je například v případě, že požadujeme osvětlení oblasti v závislosti na pohybu osob jen v určitém časovém intervalu, tedy například pouze v pracovní době. Režimy osvětlení jsou nastavitelné uživatelem pro každé svítidlo a příslušné čidlo zvlášť.

Připojení pohybových senzorů k počítači je realizáno prostřednictvím posuvných registrů typu *PISO*. Každý senzor udává svůj aktuální stav v podobě výstupní logické hodnoty pro narušený či nenarušený prostor, jenž je senzorem snímán. Tato výstupní hodnota je připojena na jeden z paralelních vstupů posuvného registru. Při požadavku aplikace na výpis dat z posuvného registru jsou údaje z paralelních vstupů vyslány do sériového portu počítače, odkud jsou načteny do paměti a dále zpracovány.

Pole logických hodnot udávající aktuální stavy pohybových čidel je využíváno nejen částí systému pro řízení osvětlení, ale také částí, která zajišťuje funkci bezpečnostního systému

objektu. Část pohybových senzorů je využívána také systémem pro řízení zavlažování venkovních prostor objektu.

Připojení jednotlivých ovládacích a snímacích prvků osvětlení je znázorněno na obrázku 6..



Obr.6: Připojení systému osvětlení

2.5.1 Modul stmívače osvětlení

K ověření správné funkce systému pro ovládání osvětlení objektu prostřednictvím řídící jednotky inteligentního domu jsem použil modul stmívače MicroDim 500. Tímto modulem by měla být v systému řízení inteligentního domu vybavena všechna svítidla u nichž je požadována regulace intenzity světla. Modul je konstruován tak, aby umožnil montáž přímo do stávající elektrické instalace objektu, díky malým rozměrům se vejde do rozvodné krabice, pod nástěnný vypínač osvětlení či přímo do vlastního osvětlovacího prvku. Tím není žádným způsobem narušen původní vzhled objektu. Modul MicroDim500 obsahuje stmívač řízený jednočipovým mikrokontrolérem, který umožňuje pracovní režim v jednom ze šesti programů. Ty jsou voleny postupným stisknutím stávajícího vypínače osvětlení. Intenzita jasu svítidla je regulována v rozmezí 0 až 98% maximálního výkonu. Pro příjemnější pocit z rozsvíceného osvětlení má modul naprogramován plynulý přechod z vypnutého stavu do plného rozsvícení (přesněji 98%). Tento přechod trvá přibližně pět sekund a přispívá k prodloužení životnosti spínaných světelných zdrojů. První předprogramovaná funkce je aktivována jedním stiskem vypínače a spočívá v plynulém rozsvícení na maximální hodnotu, jak bylo popsáno výše. Další funkcí je regulace intenzity osvětlení. Při stisknutí spínače začne světelný zdroj po dobu zmíněných pěti

sekund zvyšovat intenzitu osvětlení, při dalším stisku v tomto časovém intervalu dojde k vypnutí osvětlení a následné stisknutí vypínače způsobí rozsvícení na hodnotu intenzity, která byla nastavena v okamžiku vypnutí. Dojde-li ke třem rychlým stiskům vypínače, je aktivován třetí režim modulu stmívače. Osvětlení přejde plynule na maximální intenzitu a po třiceti minutách dojde k pozvolnému zhasnutí svítidla. Dalším režimem je imitace světelného efektu plápolajícího ohně, kdy po čtyřech rychlých stisknutích vypínače dojde k rozsvícení na polovinu maximální intenzity světla a následuje náhodné zvyšování a snižování této hodnoty. Poslední funkcí modulu je program pro opakované plynulé rozsvěcení a zhasínání svítidla. Tento režim je aktivován, dojde-li k šestinásobnému stisknutí vypínače.

Technické parametry modulu MicroDimm 500:

Rozměry: 30 x 21 x 11,5 mm
Vývody: průměr 1,5 mm, délka 10 cm
Pouzdro: ABS V-0 samozhášecí polyuretanová hmota
Napětí: 200 – 240 V / 50 Hz
Připojitelná zařízení: obyčejné či halogenové žárovky
Zatížitelnost: ohmická 15-500 W, *indukční* 15-400 W, *kapacitní* 15-250 W

Výkonový prvek modulu umožňuje regulaci zátěže až do výkonu 500W bez přídavného chlazení, při překročení této hranice je zapotřebí zajistit odvod tepla, které vzniká proudovým zatížením modulu. Instalace regulačního prvku do elektrického obvodu se provádí sériovým zapojením se zátěží přímo do cesty pracovního či fázového vodiče. V případě tzv. schodišťového vypínače lze prostřednictvím modulu regulovat osvětlení z více míst v místnosti či celém objektu. Této funkce je využito právě při spojení modulu se systémem řízení inteligentního domu, který v tomto případě pracuje jako další vypínač zapojený paralelně k vypínači v místnosti s osvětlením. Vnitřní zapojení modulu MicroDim500 umožňuje realizovat ovládání více paralelně zapojených modulů prostřednictvím jediného vypínače. Podrobnější popis zařízení je k vyhledání v publikaci [7].

2.5.2 Hlásič pohybu

Chceme-li zajistit automatické spínání osvětlení v závislosti na pohybu osob, je nutno nainstalovat do snímané oblasti senzor, který zajistí detekci pohybu a převede tuto informaci na elektrický signál. Při narušení hlídaného prostoru zpravidla následuje sepnutí zabudovaného relé, což způsobí aktivaci připojeného zařízení, kterým může být např. světelný zdroj či servomotor pro manipulaci s dveřmi.

Pohybové čidlo, které jsem použil při vývoji systému řízení inteligentního domu pro vyzkoušení požadovaných funkcí, je pasivní infračervený detektor (PIR) s označením LX48A určený pro montáž do vnitřních i vnějších prostor objektu. Tento senzor při pohybu osob v hlídaném prostoru sepne na přednastavenou dobu výstupní svorky zabudovaného relé. Součástí detektoru je obvod citlivý na intenzitu okolního osvětlení a v závislosti na nastavení aktivuje detektor pohybu. Tímto nastavením je umožněna aktivace denního a nočního režimu. Je-li jako spínané zařízení připojen např. zdroj světla, pak touto volbou nastavíme režim detektoru, kdy je čidlo pohybu aktivní pouze při poklesu intenzity osvětlení prostoru pod určitou hranici, jinak řečeno jakmile se začne stmívat, jelikož při dostatečném denním světle by aktivace umělého osvětlení postrádala smysl.

Technické údaje PIR detektoru LX48A:

Napájení: 230 V / 50Hz
Maximální zatížitelnost: 1200 W
Detekční úhel: 220°
Dosah detekce: 2-11 m (nastavitelný)
Citlivost na okolní světlo: 3-2000 LUX (nastavitelná)
Doba sepnutí výstupu: 8 sekund až 7 minut (nastavitelná)
Instalační výška: 0,5-3,5 m
Bezpečnostní krytí: IP44

Široký detekční úhel umožňuje instalaci senzoru na vnější roh objektu, k detekci pohybu pak dochází ve zbývajícím otevřeném prostoru. Pro střežení vnitřních prostor je vhodné použít stropní detektor s úhlem plných 360°, aby došlo k pokrytí největšího možného prostoru. Podrobnější popis zařízení je k vyhledání v publikaci [8].

2.5.3 Připojení k portům řídícího systému

Systém řízení inteligentního domu umožňuje regulaci osvětlení vnitřních i vnějších prostor budovy. K sériovým portům jsou připojeny výstupy pohybových senzorů rozmístěných na požadovaných místech areálu a vstupy regulačních prvků, kterými jsou buď přímo relé pro spínání osvětlení nebo moduly stmívačů rozšiřujících funkce systému o plynulou regulaci a doplňkové režimy osvětlení.

Připojení jednotlivých částí osvělení objektu je rozděleno do dvou částí podle směru toku dat na vstupní a výstupní proud informací.

Připojení vstupů modulů stmívačů k sériovému portu

K ovládání výstupních zařízení pro osvětlení je využito pouze jednoho pinu sériového portu počítače s označením *TxD*. Na tento výstup je prostřednictvím sériového rozhraní odesílán proud dat v podobě hexadecimálního číselného údaje ukončeného znaky *#13*. S využitím mikrokontroléru *PIC12C508A* ve spojení s posuvnými registry *74HC595* je docíleno převodu hexadecimálního čísla do binární podoby a tím jsou nastaveny odpovídající napěťové úrovně na výstupech posuvných registrů. Zmíněný ukončovací kód slouží pro mikrokontrolér k indikaci ukončení poudu dat ze sériové linky. Počet připojitelných modulů pro ovládání světel je určen počtem zapojených posuvných registrů. Použitý integrovaný obvod *74HC595* obsahuje 8 výstupních pinů. Podle schématu, které je znázorněno v kapitole hardwarovém řešení připojení částí systému, lze výstup mikrokontroléru rozšířit o další posuvné registry a tím rozšířit počet ovládaných světel a modulů stmívačů. Je-li počet bitů po převodu z hexadecimálního údaje na binární větší než celkový počet výstupních pinů připojených posuvných registrů, pak se přebytečné bity ignorují a jsou aktivovány pouze dostupné výstupy obvodů.

Připojení výstupů pohybových čidel k sériovému portu

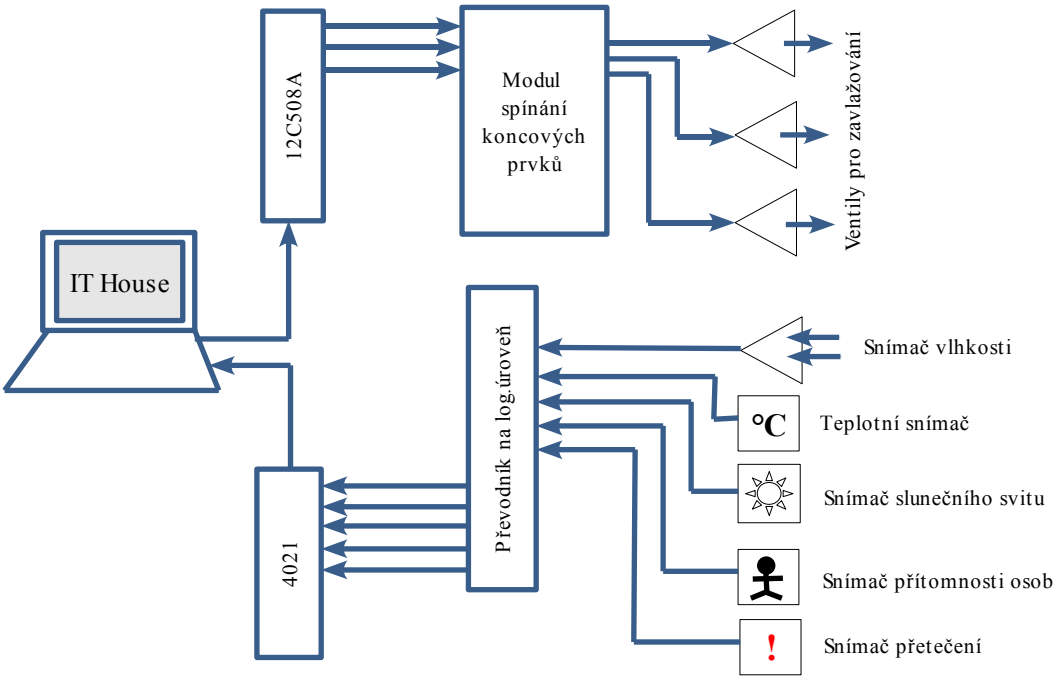
Vstupní zařízení části systému určeného pro regulaci osvětlení objektu v podobě

pohybových čidel jsou podobně jako výstupní zařízení připojena prostřednictvím posuvných registrů. Vstupní data jsou periodicky načítána z výstupů posuvných registrů a prezentována prostřednictvím uživatelského rozhraní. Nad načtenými informacemi se provedou přednastavené operace a dojde k úpravě výstupních dat a odeslání na sériový port..

K rozšíření počtu připojitelných vstupních zařízení slouží integrovaný obvod posuvného registru s označením *4021*. Tento obvod se dá ve větším počtu vzájemně propojit a tím lze získat potřebný počet pinů pro připojení jednotlivých zařízení. Načítání prostřednictvím sériového portu počítače pak probíhá pomocí signálu odeslaného ze sériového portu na vzorkovací vstup registrů s označením *CLK*. S každým odesláním signálu je z posuvného registru načtena logická hodnota příslušného pinu na paralelním vstupu registru, na který je napojeno konkrétní zařízení. Tyto operace se opět provádí periodicky a tím je docíleno okamžitého zjištění změny výstupních údajů zařízení připojeného na kterémkoliv ze vstupů posuvného registru.

2.6 Připojení zavlažovacího systému

Další částí systému inteligentního domu je ovládání zavlažování rostlin ve vnitřních i vnějších prostorách budovy. Oba systémy mají nastavitelný program, který umožňuje aktivaci či deaktivaci jednotlivých bezpečnostních prvků (čidla pohybu, teploty a slunečního záření) a akčních členů, kterými jsou elektromagnetické ventily připojené do vodovodní instalace. Rozdělení na jednotlivé okruhy umožňuje nastavení zavlažování jen vybraných částí budovy, čímž dojde k efektivnímu využití energií. Připojení k systému pro řízení inteligentního domu je znázorněno na obrázku 7.



Obr.7: Schéma monitorování a ovládání systému zavlažování

Zavlažovací systém je z pohledu centrální jednotky inteligentního domu složen ze vstupních i výstupních prvků. K rozšíření počtu připojených zařízení jsou opět použity posuvné registry, které jsou napojeny na sériový port počítače.

2.6.1 Vstupní zařízení

Vstupními prvky jsou pohybová čidla, snímače vlhkosti půdy, teploty vzduchu, intenzity slunečního záření a přetečení kapaliny. Výstupní signály snímačů jsou připojeny na vstupní piny posuvných registrů. Prostředním sériového portu je pak periodicky načítán stav těchto pinů, informace jsou zpracovány webovou aplikací a zobrazeny v systému pro řízení inteligentního domu.

2.6.2 Výstupní zařízení

Akční členy systému zavlažování v podobě elektromagnetických ventilů jsou připojeny na výstup sériového portu prostřednictvím mikrokontroléru, který umožňuje připojení a ovládání většího počtu ventilů při zachování sériové komunikace s portem počítače pouze s využitím pinu *TxD*. Vstupy elektromagnetických ventilů jsou napojeny na výstupní piny mikrokontroléru *PIC12C508A*. Na vstup tohoto obvodu je odeslána informace v hexadecimální podobě,která je po ukončení znaky *#13* převedena na bitovou mapu určující logické úrovně výstupních pinů obvodu. Aktivace akčních členů je prováděna na základě vyhodnocení vstupních informací webovou aplikací a v závislosti na zvoleném zavlažovacím programu.

2.6.3 Venkovní zavlažovací systém

Snímače vlhkosti půdy v exteriéru jsou umístěny na vhodně zvolených místech tak, aby bylo dosaženo optimálního pokrytí z hlediska odečítání množství vody obsažené v půdě. U vyústění zavlažovacího systému, která mají větší rozptyl a mohlo by dojít ke kontaktu vody s přítomnými osobami, jsou rozmístěny pohybová čidla, která v případě pohybu osob aktivují uzavírací ventil a tím zamezí nežádoucímu kontaktu. Signál z pohybových čidel je periodicky snímán systémem řízení inteligentního domu a po zpracování informací jsou provedeny nadefinované akce. Ty zpravidla spočívají v nastaveném intervalu, ve kterém se má pokus o zavlažování opakovat, případně má-li se opakovat ihned, jakmile osoby opustí hlídaný prostor. Program pro zavlažovací proces je ovlivněn také aktuální teplotou vzduchu a intenzitou slunečního záření. Snímače těchto hodnot jsou umístěny v blízkosti zavlažovacích okruhů a mají za úkol chránit rostliny před pokropením vodou na přímém slunečním světle vysoké intenzity, čímž by mohlo dojít k jejich uhynutí

2.6.4 Vnitřní zavlažovací systém

Okruhy pro zavlažování rostlin ve vnitřních prostorách budovy jsou vybaveny podobně jako okruhy v exteriéru. Rozdílem je nahrazení pohybových čidel bezpečnostními snímači přetečení, které mají za úkol deaktivovat zavlažovací ventily v případě, že dojde z jakéhokoliv důvodu k úniku kapaliny z nádob s rostlinami. Oproti venkovnímu zavlažovacímu systému s pohybovými čidly však na tomto místě není umožněno automatické opakování zavlažovacího procesu, dokud není v systému potvrzeno odstranění příčiny závady. Vnitřní systém není vybaven snímači intenzity slunečního záření.

2.6.5 Elektromagnetické ventily

Akční členy v podobě elektromagnetických ventilů jsou spojeny s příslušnými zesilovacími prvky (relé či tranzistorové spínače), které jsou schopny zajistit sepnutí elektromagnetických ventilů signálem vyslaným na vstup zesilovacího prvku v podobě logické úrovně a jsou dimenzovány na dostatečnou proudovou zátěž.

2.7 Připojení bezpečnostního systému

Systém řízení inteligentního domu umožňuje připojení stávajícího zabezpečovacího zařízení instalovaného v objektu. Prostřednictvím posuvných registrů lze připojit a monitorovat výstupy ústředny zabezpečovacího systému a nastavit požadované akce, které jsou vykonány řídící jednotkou inteligentního domu. Tato funkce systému je samozřejmě přístupná jen za předpokladu, že použitá bezpečnostní ústředna podporuje komunikaci s externím zařízením pro čtení výstupních dat. Pokud ústředna podporuje ukládání stavových informací s časovým údajem do vnitřní paměti a následné poskytnutí těchto informací jako výstupní data, systém řízení inteligentního domu umožňuje tato data načíst a uložit pro další zpracování. Připojení konkrétního zabezpečovacího systému musí být vyřešeno individuálně pro daný objekt, nicméně systém řízení inteligentního domu je v základní konfiguraci připraven na snímání deseti různých režimů bezpečnostní ústředny. V následujícím textu jsou popsány režimy, které jsou charakteristické pro většinu zabezpečovacích zařízení. Systém řízení inteligentního domu aktivně nezasahuje do stávající instalace bezpečnostního zařízení, jde pouze o monitorování stavu systému. Z tohoto důvodu je možné přidělit libovolným režimům konkrétní bezpečnostní ústředny jednotlivé vstupy posuvných registrů a následně pomocí popisu ve webové aplikaci spojit získané informace s příslušnými prvky uživatelského rozhraní.

Základním režimem většiny bezpečnostních systémů je tzv. režim *disarmed*, kdy není zabezpečení objektu aktivní a systém nereaguje na narušení hlídané oblasti. Do tohoto režimu přejde bezpečnostní zařízení zpravidla po přijetí bezpečnostního kódu, který může být zadán ručně na klávesnici bezpečnostního zařízení nebo se může jednat například o plovoucí kód dálkového ovladače. Deaktivace bezpečnostního systému závisí na použitém typu zařízení, upřednostňovaném řešení výrobce či požadavcích zákazníka.

Dalším režimem, který může být vyhodnocován řídící jednotkou inteligentního domu, je režim *standby*. Pokud je zařízení pro aktivaci bezpečnostního systému instalováno v podobě klávesnice či spínače ve střeženém prostoru, musí bezpečnostní zařízení podporovat provozní režim podobný režimu *standby*. Aktivace bezpečnostního systému pak probíhá tak, že po zadání bezpečnostního kódu přejde systém do režimu monitorování bezpečnostních prvků až po nastaveném časovém intervalu, který je určen k tomu, aby osoba zadávající kód mohla opustit střežený prostor. Kdyby byl bezpečnostní systém spuštěn ihned, došlo by k poplachu vlivem pohybového čidla, které zaregistrovalo pohyb osoby ve střeženém prostoru.

Jedním z aktivních režimů zabezpečovacího systému je režim *armed*. V případě aktivace bezpečnostního systému je začne pracovat ústředna v režimu hlídání střežených prostor prostřednictvím monitorování bezpečnostních snímačů. V tomto režimu jsou tedy všechna bezpečnostní čidla aktivní a při narušení hlídané oblasti dojde k poplachu a dalším nastaveným akcím podle vybavení zabezpečovacího systému (volání na telefonní číslo či zaslání sms zprávy, kontaktování systému centrální ochrany apod.). Pokud je narušen prostor, který obsahuje prvek pro oprávněnou deaktivaci bezpečnostního sytému (zpravidla klávesnice pro zadání kódu), potom poplachu předchází režim *pre-alarm*, který je popsán dále.

K režimu *armed* bývá v zabezpečovacích systémech často implementován režim s velice podobným provozním nastavením. Jedná se o režim *armed-home*, který pracuje na stejném principu jako režim *armed*, pouze s tím rozdílem, že monitoruje stav pouze vybraných bezpečnostních prvků. Využití tohoto režimu je v případě, že v některých částech objektu je umožněn pohyb osob či manipulace se zabezpečenými prvky (dveře, okna apod.), ale ve vybraných prostorách je vyžadováno střežení před narušením bezpečnostní zóny. Může se jednat o sklad, který je součástí prodejny či vstupní halu, garáž nebo hostinský pokoj rodinného domu.

Režim *pre-alarm* je podobný jako režim *standby*, pouze s tím rozdílem, že jednotlivé kroky jsou v opačném pořadí. To znamená, že je-li bezpečnostní systém v režimu *armed* či *armed-home*, pak při narušení střeženého prostoru s prvkem pro deaktivaci systému nedojde k vyvolání poplachu okamžitě, ale až po nastaveném časovém intervalu. Toto zpoždění je určeno k zadání bezpečnostního kódu příchozí osobou a deaktivaci bezpečnostního systému.

Dojde-li k narušení hlídané oblasti v režimu *armed* či *armed-home*, bezpečnostní systém přejde do režimu *alarm* a dojde k vyvolání poplachu v podobě zvukové, vizuální či jiné signalizace. Další možností může být akivace telefonního spojení s nastavenými telefonními čísly spojená s odposlechem narušené oblasti, odeslání sms zprávy či navázání komunikace s bezpečnostní službou. Režim *alarm* je aktivován také v případě, že v režimu *pre-alarm* nedošlo v časovém intervalu k deaktivaci bezpečnostního zařízení. Přejde-li ústředna zabezpečovacího systému do tohoto režimu, mohou následovat další přednastavené akce, které závisí na stupni zabezpečení objektu. Příkladem může být okamžitá aktivace bezpečnostních zámků, zamezení přístupu k vybraným oblastem (včetně přístupu autorizovaných osob) nebo při vysokém stupni zabezpečení také spuštění ochranných prvků přístupových míst jako jsou například mříže či kovové rolety.

2.7.1 Bezpečnostní systém Jablotron

Připojení stávajícího bezpečnostního systému jsem neměl možnost ověřit prakticky, jelikož jsem neměl kompletní a hlavně kvalitní zabezpečovací systém k dispozici. Proto jsem se inspiroval komplexním řešením zabezpečení využitím systému Oasis firmy Jablotron, která svými letitými zkušenostmi zajišťuje bezesporu jedny z nejspolehlivějších systémů v oblasti zabezpečení majetku.

Systém Oasis je realizován v podobě stavebnice složené z navzájem kompatibilních modulů. Srdcem bezpečnostního systému Oasis je základní deska JA-82K se čtyřmi drátovými vstupy a padesáti adresami pro periferie poskytující vysokou variabilitu konfigurace zabezpečení objektu díky možnosti rozšiřujících modulů. Tyto moduly disponují přídavnými funkcemi jako je připojitelnost bezdrátových senzorů, rozšíření počtu drátových vstupů, komunikace prostřednictvím technologie Bluetooth, sítě Ethernet, GSM a pevné telefonní linky.

Technické parametry ústředny JA-82K:

Napájení: 230 V / 50 Hz
Záložní zdroj: 12 V, 2,2 Ah
Externí poplach: výstup spíná na GND, zatížení max. 0,5 A
Interní poplach: výstup spíná na GND, zatížení max. 0,5 A
Programovatelné výstupy: PGX, PGY, max. 0,1 A, spínání na GND
Vnitřní paměť: 255 událostí s časovým údajem
Pracovní kmitočet: 868 MHz
Montáž: vnitřní prostředí, teplota -10 až 40 °C

Ovládání jednotlivých funkcí a nastavení konfigurace bezpečnostního systému řady Oasis vybaveného ústřednou JA-82K probíhá prostřednictvím obslužného software, který je součástí dodávané ústředny a také je zdarma ke stažení z internetových stránek firmy Jablotron. Spojení ústředny s počítačem může být uskutečněno prostřednictvím bezdrátové technologie Bluetooth, v takovém případě je nutno vybavit ústřednu modulem JA-80BT. Použitím dalšího rozšiřujícího modulu JA-80V je k dispozici připojení ústředny do sítě Ethernet. Tento modul poskytuje také komunikaci ústředny prostřednictvím sítě GSM s bránou GSMGateway.

Nastavení a monitorování stavu ústředny tak může probíhat na dálku s využitím serveru *GSMLink.cz.*Podrobnější popis zařízení je k vyhledání v publikaci [9].

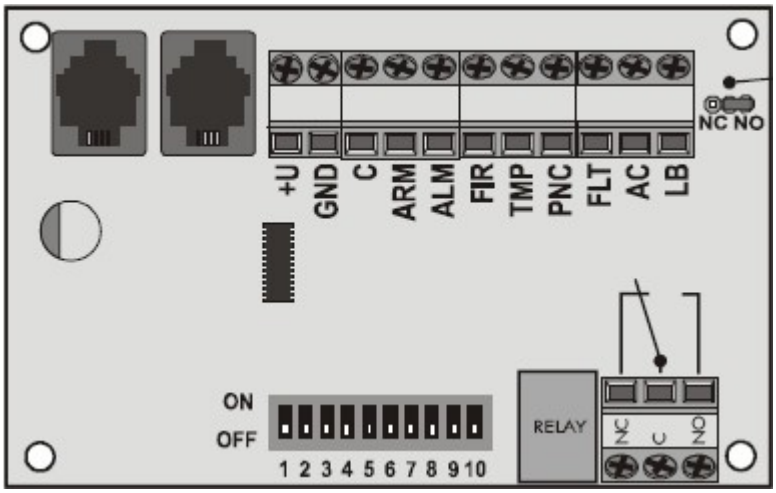
2.7.2 Rozšiřující modul JA-68

Nejdůležitější částí pro monitorování ústředny systémem řízení inteligentního domu je modul s označením JA-68 poskytující informace o stavu bezpečnostního systému v podobě nastavitelných logických úrovní polovodičových výstupů. Tato forma informace je vhodná pro připojení k posuvným registrům řídící jednotky inteligentního domu a k prezentaci získaných dat v uživatelském rozhraní.

Technické parametry:

Napájení: 12 V (připojení ze základní desky)
Proudový odběr v klidovém stavu: 4 mA
Maximální proudový odběr: 50 mA
Výstupy: 8 x polovodičových, 1x relé
Zatížitelnost polovodičových výstupů: max. 200 mA / výstup
Zatížitelnost relé: max. 1 A / 60 V
Minimální doba sepnutí výstupů: 10 s

Podrobnější popis zařízení je k vyhledání v publikaci [9].



Obr.8 : Modul JA-68

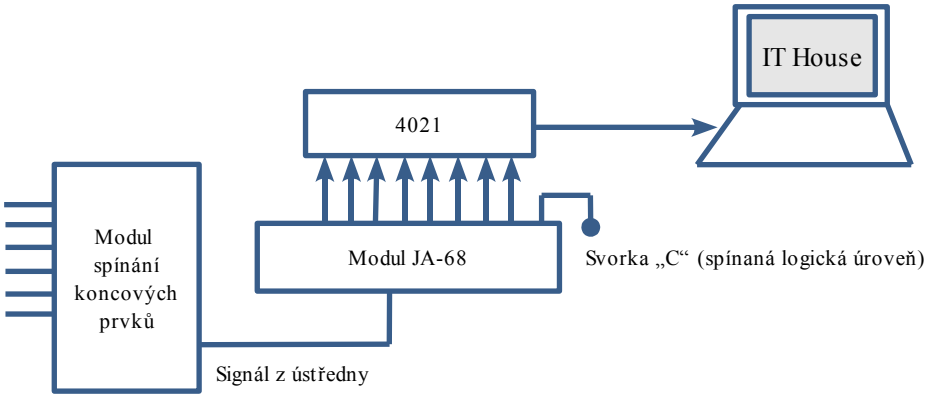
Výstupní polovodičové prvky jsou spínány se svorkou s označením „C“, na kterou je zapotřebí připojit napěťovou úroveň požadovanou na výstupu v okamžiku sepnutí příslušného polovodičového prvku. Význam jednotlivých výstupů po připojení k základní desce bezpečnostního systému je zapsán v následující tabulce.

Označení	Funkce
+U	Kladný pól napájení ze sběrnice (omezený na 200 mA)
GND	Záporný pól napájecího napětí
C	Společná svorka všech polovodičových výstupů
ARM	Stav zajištěno cokoliv (A nebo B nebo ABC)
ALM	Poplach narušením zpožděnou, okamžitou nebo následně zpožděnou smyčkou
FIR	Požární poplach (snímačem kouře nebo úniku plynu)
TMP	Sabotáž systému, narušení Tamper kontaktu periferie
PNC	Tísňový poplach
FLT	Všeobecná porucha v systému, ztráta periferie nebo porucha záložního akumulátoru
AC	Výpadek síťového napájení 230V
LB	Slabá baterie v periferii (detektor, klávesnice, siréna)

Obr.9 : Tabulka přípojných svorek modulu JA-68

Propojením svorky „C“ s napájecím napětím modulu (tedy se svorkou „+U“) lze získat na výstupech v okamžiku aktivace hodnotu napětí 12 V. Jednotlivé výstupy jsou propojeny s posuvnými registry systému řízení inteligentního domu a při aktivním výstupu je hodnota napětí přenesena na komunikační port řídící jednotky a dále zpracována aplikací. Ke každému výstupu bezpečnostního systému (konkrétně tedy výstupu modulu JA-68) lze pak v uživatelském rozhraní připojit popis události, o kterou se jedná a nadefinovat další reakce systému.

Systém řízení inteligentního domu je k bezečnostnímu systému připojen podle schématu na obrázku 10. Připojení zabezpečovacího systému *Jablotron* do sériového portu počítače je zprostředkováno výstupními obvody modulu *JA68*.



Obr.10: Připojení bezpečnostního systému

Připojení pinů modulu JA-68

Modul JA-68 poskytuje informace o provozním režimu zabezpečovacího zařízení. Veškerá komunikace s modulem je tedy jednosměrná. Jednotlivé výstupy jsou připojeny na vstupní piny posuvného registru. Modul JA-68 umožňuje nastavení logické úrovně, která bude vysílána na výstupech v případě aktivace. Všechny výstupy spínají ke svorce s označením „C“ s tím, že pomocí propojky JP1 lze nastavit logiku spínání na rozpínací nebo spínací. To znamená, že v případě propojení JP1 na pozici NO (spínací logika) bude v případě aktivace na příslušném výstupu hodnota napětí stejná jako na svorce „C“, v klidovém režimu je výstupní pin spojen se zemnící svorkou GND. V opačném případě, pokud dojde k propojení JP1 do režimu NC, pak je logika spínání nastavena do rozpínacího režimu. V tomto případě je na výstupech v klidovém stavu napětí stejné jako na svorce „C“ a v případě aktivace je konkrétní výstup připojen na GND. V případě aktivního výstupu pak můžeme u spínací logiky uvažovat výstupní hodnotu jako log 1, u rozpínací pak log 0.

V systému pro řízení inteligentního domu jsou výstupy nastaveny na rozpínací logiku, za aktivní výstup je tedy považován výstup s logickou úrovní 0. Výstupy modulu ARM, ALM, FIR, TMP, PNC, FLT, AC a LB jsou připojeny přes napěťové děliče k jednotlivým vstupním pinům posuvného registru 4021. Obsah tohoto registru je po sériové lince převeden do portu počítače a vyhodnocen aplikací. Načítání aktuálního stavu jednotlivých vstupních linek posuvného registru je periodicky opakováno. Veškerá komunikace včetně aktuálního obsahu registru v podobě binárního čísla je zaznamenána spolu s časovým údajem pořízené informace do souboru *security.log*. Tento soubor je pak použit při diagnostice narušení i bezpečnostních režimů zabezpečovacího systému. Spolu se záznamem do souboru je vstupní informace načtené ze sériového portu odeslána webové aplikaci pro další zpracování. Uživatelské rozhraní umožňuje přehledné zobrazení jednotlivých částí systému, které jsou pomocí inteligentního domu monitorovány.

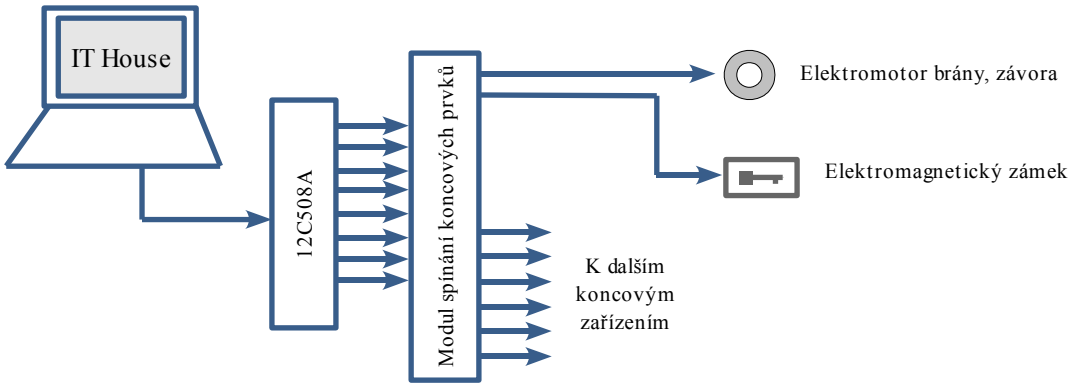
Ve spojení s pohybovými čidly, která jsou určena pro aktivaci osvětlení areálu, je umožněno aktivovat poplachové zařízení nezávislé na samostatném zabezpečení objektu. Pokud jsou tato pohybová čidla nastavena v režimu „armed“, dojde při narušení hlídaného prostoru nejen k vyhodnocení zabezpečovací ústřednou nezávislého bezpečnostního zařízení, ale také k aktivaci volitelných prvků systému pro řízení inteligentního domu. Tímto způsobem lze například vyvolat tichý poplach s upozorněním obsluhy, případně zamezit selhání samostatného

bezpečnostního zařízení při jeho zneškodnění narušitelem. Volitelně lze také aktivovat jednotlivá osvětlení objektu v závislosti na konfiguraci vstupních dat z pohybových senzorů. Pro načtení informací z těchto čidel je využito vstupních dat periodicky získávaných pro část systému řízení inteligentního domu určenou k osvětlení objektu. Tato část je využita také pro případnou aktivaci jednotlivých osvětlení v případě narušení hlídaného prostoru.

2.7.3 Ovládání zámků prostřednictvím BT technologie

Systém řízení inteligentního domu umožňuje ovládání elektromagnetických zámků a elektromotorů, kterými jsou vybaveny příslušné vstupní či výstupní prostory objektu. Tyto prvky jsou ovládány přímo z uživatelského rozhraní nebo prostřednictvím bezdrátové technologie *bluetooth*. Aktivace či deaktivace příslušného zámku nebo motoru je chráněna provozním režimem a konfigurací zabezpečovacího systému. V případě manipulace z uživatelského prostředí je vždy ověřen režim zabezpečovacího zařízení a výstupní hodnoty pohybového čidla v blízkosti zámku či elektromotoru. V závislosti na vyhodnocení a aktuální konfiguraci jsou provedeny uživatelem požadované akce.

V základním nastavení je výsledkem úspěšného požadavku překlopení zámku do obrácené polohy než je aktuální, v případě elektromotoru ovládajícího například bránu dojde k přetočení do opačného stavu, tedy k otevření uzavřené brány a naopak. Systém lze však nakonfigurovat i tím způsobem, že po odeslání kódu bude přidružené osvětlení aktivováno, deaktivováno nebo nastaveno na uloženou intenzitu světla. Podobným způsobem lze také například deaktivovat pohybová čidla v budově či v areálu.



Obr.11: Ovládání zámků a elektromotorů

3 Programové vybavení

Jako operační systém byl použit Microsoft Windows XP Professional SP3 s instalací platformy .NET Framework 2.0 pro podporu technologie ASP.NET a jazyka C#, v němž je celá aplikace naprogramovaná. K vývoji systému bylo použito prostředí Microsoft Visual Studio 2008.

První spuštění aplikace je prováděno za asistence správce systému, jelikož vyžaduje určitá nastavení v závislosti na konkrétní konfiguraci celého systému. Pro reprezentaci vstupních a výstupních hodnot systému je zvoleno pole výstupních dat pro nastavení jednotlivých podsystémů a pole vstupních dat, načtených z jednotlivých snímaných prvků těchto systémů. Konfiguračním souborem pro správnou funkci aplikace je soubor *web_app.config*. V tomto souboru je při prvním spuštění aplikace uložena konfigurace systému, která je nutná pro pozdější případné problémy při chodu aplikace, jako je například přechod do nouzového režimu aplikace či restartování počítače.

Při každé významnější akci prováděné uživatelem je do souboru web_app.*log* zapsán aktuální čas a identifikační název akce. Tento soubor slouží k monitorování chodu aplikace a k případné identifikaci a následnému odstranění vzniklého problému.

3.1 Webový server

3.1.1 Apache HTTP server

Funkce webové aplikace pro řízení inteligentního domu jsou poskytovány a zpracovávány prostřednictvím webového serveru Apache. Pro realizaci systému byl použit HTTP server Apache ve verzi 2.2.15.

Instalace Apache

Instalační program webového serveru Apache poskytuje základní konfigurační možnosti pro počáteční nastavení serveru. Při instalaci byla zvolena doména a název serveru, cesta pro nakopírování souborů serveru a také adresář, kde se bude nacházet webová aplikace systému pro řízení inteligentního domu, např.: *„C:\dev\www “*.

Po úspěšné instalaci je nutno složku s webovou aplikací nakopírovat do výše zmíněného adresáře. Následujícím krokem je instalace modulu, který zajistí podporu technologie ASP.NET na webovém serveru Apache. Podrobnější informace o serveru Apache jsou k vyhledání v publikaci [10].

3.1.2 Modul Mod_AspDotNet

Abychom mohli použít technologii Microsoft ASP.NET ve spojení s webovým serverem Apache, je zapotřebí nainstalovat modul, který toto rozšíření umožní. Požadavky pro správnou funkci modulu jsou samozřejmě korektně nainstalovaný webový server Apache (ve verzi 2.2 a vyšší), dále pak instalace .NET Framework ve verzi minimálně 1.1 a pro operační systém Windows XP minimálně Service Pack 1.

Pro realizaci systému řízení inteligentního domu byla použita verze modulu 2.2.14. Instalační program modulu si vyhledá umístění instalace webového serveru a po úspěšném zkopírování pootřebných souborů můžeme přistoupit k nastavení serveru pro zpracování webových stránek využívajících technologii ASP.NET.

Nastavení serveru spočívá v přidání modulu do konfiguračního souboru *httpd.conf* a definování přístupu k souborům webové aplikace systému řízení inteligentního domu. Na konci konfiguračního souboru webového serveru jsou přidány instrukce pro připojení modulu a nastavení přístupu k webové aplikaci.

Prvním krokem je připojení modulu:

```
LoadModule aspdotnet_module "modules/mod_aspdotnet.so"

AddHandler asp.net asax ascx ashx asmx aspx axd config cs csproj licx rem resources
resx soap vb vbproj vsdisco webinfo
```

Následuje nadefinování cesty k adresáři ITHouse, který obsahuje webovou aplikaci:

```
<IfModule mod_aspdotnet.cpp>

    AspNetMount /ITHouse "c:/dev/www/ITHouse"
```

Namapování požadavků na zobrazení stránek webové aplikace do adresářové struktury:

```
    Alias /ITHouse "c:/dev/www/ITHouse"
```

Nastavení přístupu a určení výchozí stránky:

```
    <Directory "c:/dev/www/ITHouse">
        Options FollowSymlinks ExecCGI
        Order allow,deny
        Allow from all
      DirectoryIndex index.htm index.aspx
    </Directory>
</IfModule>
```

V sekci *<Directory>* je pomocí instrukce *Allow from all* implicitně nastaven přístup pro všechny požadavky z libovolné IP adresy. Za touto instrukcí lze explicitně nastavit zamezení přístupu pro konkrétní adresy prostřednictvím instrukce *Deny from* , která je následována IP adresou. Je-li zapotřebí odmítnout požadavky přicházející ze zdroje s adresou 10.0.0.1, stačí zadat instrukci *Deny from 10.0.0.1* a tyto požadavky budou zamítány a nedojde k jejich zpracování. Podobně lze implicitně zakázat přístup ze všech IP adres, prostřednictvím instrukce *Deny from all*, spolu s explicitním povolením jen určité IP adresy instrukcí *Allow from* (např.: *Allow from 10.0.0.1*). Po uložení změn v konfiguračním souboru a restartování webového serveru je již umožněno zpracování stránek ASP.NET webovým serverem Apache. Informace k popisu modulu pro podporu ASP.NET byly čerpány z publikace [11].

3.2 Webové rozhraní

Na počítači, který zajišťuje řízení inteligentního domu, je spuštěn webový server Apache. Tento server je po instalaci příslušné modifikace a nastavení konfiguračních souborů schopen spolupracovat s technologií ASP.NET.

3.2.1 Bezpečnostní aspekty technologie ASP.NET

Platforma .NET Framework poskytuje široké spektrum možností jak zabezpečit vyvíjený softwarový produkt. Proces zajištění přístupu k funkcím aplikace pouze pověřeným osobám sestává ze dvou hlavních kroků – autentizace a autorizace.

3.2.1.1 Autentizace uživatele

Proces autentizace spočívá v ověření identity odesílatele požadavku obdrženého webovým serverem. Tímto procesem je zjištěno, zda je uživatel opravdu tím, za koho se vydává. Technologie ASP.NET umožňuje nastavit jednu ze čtyř možností autentizace – *windows, passport, forms* nebo *none.*

Při použití autentizace typu *windows* je uživatel ověřen podobným způsobem jako při přihlašování do systému Windows. Je tedy zobrazeno okno pro zadání uživatelského jména a hesla a po potvrzení jsou údaje zpracovány přímo serverem. ASP.NET v tomto případě přímo do vlastního ověření uživatele nezasahuje a způsob ověření identity závisí na možnostech poskytovaných serverem. Veškeré požadavky na zobrazení či manipulaci s daty jsou pak zpracovávány v kontextu přihlášeného uživatele. Tento způsob autentizace není vhodný pro použití v síti internet, jelikož uživatel musí být zaregistrován právě na serveru či v doméně. Využití takové autentizace je pak zejména v intranetových sítích.

Autentizace v podobě režimu *passport* zajišťuje ověření identity uživatele proti databázi služby *Microsoft Passport*. Při ověřování se webová aplikace spojí s touto službou a ověří uživatelem zadané přihlašovací údaje. Chceme-li tuto formu autentizace použít, musíme na server nainstalovat sadu *.NET Passport SDK* a provést registraci webového serveru u služby *Microsoft Passport*. Hlavní myšlenkou této služby je použití jednotných přihlašovacích údajů uživatele pro autentizaci na zaregistrovaných webových serverech. Zpřístupnění stránek poskytovaných těmito webovými servery je pak prováděno bez opakovaného ověřování identity uživatele, jelikož uživatel se pohybuje v důvěryhodném prostředí serverů zaregistrovaných u služby *Microsoft Passport*.

Režim ověření identity uživatele prostřednictvím autentizace typu f*orms* poskytuje vysokou variabilitu při realizaci zabezpečení webové aplikace. Jedná se o tzv. *formulářovou autentizaci*, která již není prováděna na úrovni webového serveru, ale identifikační údaje uživatele jsou zpracovány přímo webovou aplikací. Programátor této aplikace má pak přehled nad veškerými uživateli, kteří se do systému přihlašují. Prostřednictvím vlastní naprogramované logiky je schopen nastavit celkové řízení procesu ověřování identity.

Čtvrtou možností autentizace je režim *none,* pomocí které je možno nastavit aplikaci tak, aby žádnou autentizaci neprováděla.

Pro zabezpečení webové aplikace pro řízení inteligentního domu byla zvolena autentizace typu *forms* z důvodu zmíněné flexibility při návrhu a implementaci zabezpečení aplikace.

Nastavení autentizace v režimu *forms*

Prvním krokem v případě použití režimu *forms* je povolení přístupu k serveru všem uživatelům, jedná se o takzvaný anonymní přístup k serveru. Pokud by nebyl server nastaven pro anonymní přístup, nemohli by k němu přistupovat uživatelé jiných systémů než *Microsoft Windows,* nicméně v tom případě bychom mohli použít přímo autentizaci typu *Windows*. Následující úpravou souboru *web.config* sdělíme systému, že pro ověření uživatele využijeme formulářové autentizace.

```
<authentication mode="Forms">
  <forms  name="login"
       loginURL="login.aspx"
       protection="All"
       timeout="30"
       path="/" />
</authentication>
```

Při úspěšném ověření identity uživatele je na straně klienta uložen soubor *cookie*, který informuje server o tom, že identita uživatele již byla ověřena a při dalších požadavcích na zobrazení zabezpečeného obsahu zamezí opětovnému vyžádání autentizace uživatele. Název a místo uložení tohoto souboru *cookie* je definován proměnnou *name* a *path* v nastavení autentizace *Forms* v konfiguračním souboru. Proměnná *loginURL* označuje adresu stránky, jenž obsahuje formulář pro zadání přihlašovacích údajů. Na tuto stránku bude pesměrován uživatel, jehož identita nebyla zatím ověřena a nebyl tedy nalezen příslušný soubor *cookie*. Proměnná *protection* obsahuje nastavení pro zabezpečení autentizačního soubrou *cookie*. Hodnota této proměnné je ponechána ve stavu *All*, toto nastavení určuje, že je soubor následně zakódován a podepsán použitím hashovací funkce pro maximální zabezpečení proti zneužití. Doba platnosti souboru *cookie* je nastavena proměnnou *timeout*. Výchozí hodnota je 30 minut, zkrácením této doby můžeme nastavit požadavek na častější obnovování autentizačního souboru a tím zkrátit čas pro vypršení úspěšné autentizace uživatele.

Ověření identity uživatele

Při požadavku na zobrazení zabezpečeného obsahu je uživatel přesměrován na stránku obsahující prvky pro zadání přihlašovacích údajů. Po zadání těchto údajů závisí další postup přihlašování právě na programátorovi, který určí jednotlivé kroky pro zpracování přihlašovacích údajů uživatele. Na počátku je vhodné ověřit, zda bylo přihlašovací jméno a heslo zadáno ve správném formátu. Platforma *.NET Framework* poskytuje několik funkčních prvků pro kontrolu správného tvaru zadaných údajů, jedná se o tzv. validátory. Jsou-li přihlašovací údaje úspěšně zkontrolovány z hlediska správného formátu, následuje zpracování údajů podle naprogramované logiky. Přihlašovací jméno a heslo je předloženo obslužné metodě a porovnáno s daty použitého úložiště. Jsou-li přihlašovací údaje shodné s uloženým záznamem, uživateli je umožněn přístup do zabezpečené oblasti webové aplikace. V opačném případě je uživatel přesměrován zpět na stránku s formulářem pro přihlášení. Metoda pro zpracování údajů pro přihlášení využívá kolekci *System.Web.Security.FormsAuthentication*, způsob použití je v následující ukázce a spočívá v předložení uživatelského jména a hesla metodě *Authenticate* této kolekce, která na základě úspěšnosti ověření vyhodnotí, zda bude uživateli umožněn přístup k zabezpečenému obsahu.

```
If (FormsAuthentication.Authenticate(login, password))
        {
           FormsAuthentication.RedirectFromLoginPage(login, false);
        }
```

Metoda *Authenticate* vrací hodnotu *true* právě tehdy, je-li uživatelské jméno a heslo nalezeno mezi uloženými údaji. V takovém případě zajistí metoda *RedirectFromLoginPage* ze stejné kolekce zpřístupnění zabezpečené oblasti tomuto ověřenému uživateli. Údaje pro přihlášení uživatelů mohou být uloženy několika způsoby, pokaždé jde však v rámci kolekce *System.Web.Security.FormsAuthentication* a příslušných ověřovacích metod o stejný způsob konečného ověření, kde jsou jako parametry metody *Authenticate* použity přihlašovací údaje v podobě jména a hesla. Pro úplnost je potřeba ještě dodat význam druhého parametru metody *RedirectFromLoginPage*, který určuje, zda má být autentizační soubor *cookie* perzistentního typu či nikoliv, tedy má-li být autentizace uživatele trvalá s časově neomezenou platností a s přetrváním platnosti i po restartování prohlížeče nebo jen dočasná s ukončením platnosti po vypršení nastaveného časového intervalu či uzavření prohlížeče.

Úložiště přihlašovacích údajů

Jednou z možností kam uložit přihlašovací údaje uživatelů je použít přímo konfigurační soubor *web.config* webové aplikace. Uživatelská jména a hesla jsou pak uložena v sekci <*forms*> do podsekce <*credentials*> následujícím způsobem.

```
<credentials passwordFormat="MD5">
        <user name="login" password="heslo" />
</credentials>
```

V sekci *user* jsou uloženy platné přihlašovací údaje jednotlivých uživatelů pro přístup do zabezpečené oblasti webové aplikace. Uložené heslo může být zašifrováno algoritmy *SHA1* či *MD5*, nastavení je určeno hodnotou proměnné *passwordFormat*. V případě, že není požadováno šifrování hesla, nastavíme proměnnou na hodnotu *Clear*, čímž dojde k uložení hesla v původním textovém formátu.

Pro uložení přihlašovacích údajů a jejich zpětného načtení v případě požadavku na autentizaci je možno použít i jiná úložiště, jako je např. soubor typu *XML* či *databáze SQL*. Výsledný způsob ověření identity uživatele však zůstává stejný, jak je již popsáno výše. Součástí je pouze práce s příslušným datovým zdrojem při prohledávání údajů o uživatelích a porovnávání s údaji zadanými uživatelem při požadavku na přihlášení prostřednictvím formuláře.

3.2.1.2 Autorizace uživatele

Dosud provedená nastavení v souboru *web.config* týkající se autentizace ještě nestačí pro zabránění nepovolaným uživatelům v přístupu na stránky webové aplikace. Bez dalšího zabezpečení v podobě *autorizace uživatelů* budou stránky přístupné všem uživatelům bez rozdílu identity, jelikož webová aplikace *ASP.NET* má výchozí určení přístupu nastaveno právě na anonymní přístup, tedy zpřístupnění všem uživatelům.

Autorizace uživatelů úzce souvisí s procesem autentizace při zajištění bezpečnosti webové aplikace. Po úspěšné autentizaci uživatele je potřeba ověřit, zda má uživatel oprávnění k

přístupu do zabezpečené oblasti. Proces autorizace se už nezabývá tím, zda má uživatel skutečně identitu, za kterou se vydává, ale zda již autentizovaná identita disponuje přístupovými právy k určitému zdroji informací, jinými slovy zda je přihlášený uživatel oprávněn k zobrazení stránky obsahující zabezpečená data případně k zásahu do nastavení, jenž stránka umožňuje.

Nastavení autorizace v technologii ASP.NET

Chceme-li umožnit přístup ke stránkám webové aplikace pouze těm uživatelům, u nichž proběhla úspěšná autentizace v předchozím kroku zabezpečení, musíme zakázat přístup všem anonymním uživatelům. Důvodem je, jak již bylo zmíněno, implicitní nastavení aplikace, které spočívá v umožnění přístupu všem uživatelům, kteří si vyžádají zabezpečené informace. Natavení autorizace se provádí opět v konfiguračním souboru *web.config* webové aplikace, stejně jako tomu bylo v případě autentizace uživatelů. V sekci <*system.web*> vytvoříme podsekci <*authorization*>, kam vložíme požadované pravidlo pro autorizaci uživatelů.

```
<system.web>
        <authorization>
                <deny users="?" />
        </authorization>
</system.web>
```

Tímto nastavením je zakázán přístup ke stránkám webové aplikace všem uživatelům, kteří neprošli úspěšnou autentizací. Pokud se takový uživatel pokusí zobrazit zabezpečenou stránku, pak jej modul pro autentizaci automaticky přesměruje na stránku určenou pro přihlášení, jejíž adresa je zadána jako hodnota proměnné *loginUrl* v sekci <*authentication*><forms> konfiguračního souboru *web.config*.

Sestavení pravidel pro přístup ke zdrojům

V sekci <*authorization*> můžeme provést také nastavení přístupu pouze konkrétním uživatelům. Postup je pak takový, že nejprve vytvoříme pravidla pro zpřístupnění a blok zakončíme pravidlem pro zamezení přístupu všem uživatelům. Ověřování pravidel probíhá odshora dolů a již akceptovaná pravidla se dalším načteným pravidlem v případě logické kolize významu neruší. Následující úpravou souboru *web.config* umožníme přístup uživatelům *Roy* a *Moss*, avšak všem ostatním je přístup zamítnut.

```
<system.web>
        <authorization>
                <allow users="Roy" />
                <allow users="Moss" />
                 <deny users="*" />
        </authorization>
</system.web>
```

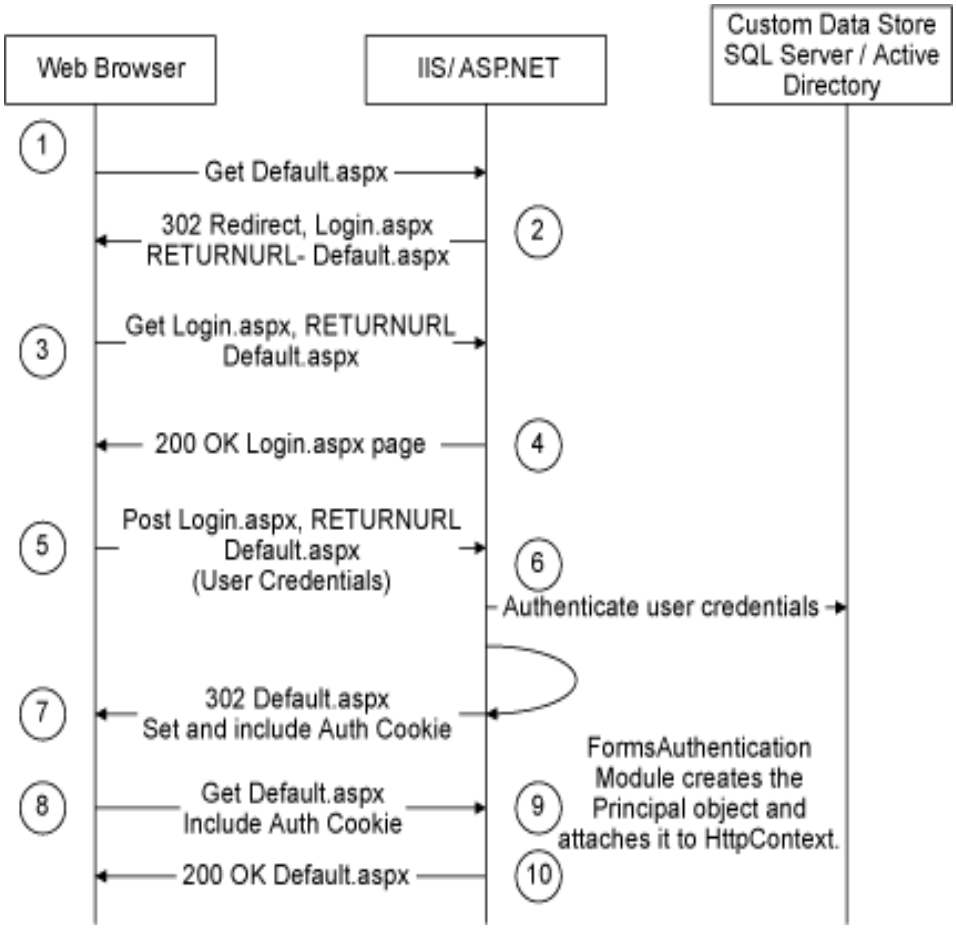
V tomto případě je však na rozdíl od předchozího nastavení zamezen přístup úplně všem uživatelům včetně těch, kteří byli úspěšně autentizováni. Uživatel *Roy* bude tedy systémem akceptován a zabezpečené informace, které požadoval budou zobrazeny, podobně tomu bude

také v případě požadavku od uživatele *Moss*. Přijde-li požadavek na zabezpečenou stránku např. od uživatelky *Jenn*, která je sice zaregistrována jako platná identita webové aplikace, výsledné zobrazení nebude akceptováno. Uživatelka sice projde úspěšnou autentizací, avšak není explicitně uvedena v sekci pro autorizaci a její přístup k danému zdroji je tedy zamítnut. Jak je nesjpíš zřejmé, symbol „*“ (hvězdička) označuje všechny uživatelské účty a „?“ v předchozím zápisu má význam anonymní identity.

V následujícím diagramu jsou znázorněny jednotlivé kroky při zpracování autentizace spolu s ověřením oprávnění k přístupu uživatele k požadovanému obsahu stránky (autorizací) využitím funkcí technologie ASP.NET . Komunikace probíhá mezi webovým klientem a serverem, na obrázku je jako webový server znázorněn Internet Information Server, komunikace se serverem Apache však probíhá na stejném principu .

Popis komunikace webového klienta a webového serveru

Zpracování požadavku na zobrazení zabezpečené stránky je znázorněno na obr.:xx. Diagram je v anglickém jazyce - části práce jsou použity v dokumentaci systému, který je v angličtině.



Obr.12: Zpracování požadavku na zobrazení zabezpečené stránky (zdrojem je [13])

Postup při zpracování požadavku

1. Nejprve je vyslán požadavek uživatele na zobrazení zabezpečeného obsahu, v tomto případěj jde o *stránku Default.aspx*. Webová aplikace podle pravidel v souboru *web.config* zjistí, že anonymní přístup k obsahu je zakázán.
2. Následuje hledání souboru *cookie* pro ověření identity uživatele. Pokud tento soubor neexistuje, uživatel je přesměrován na stránku s formulářem pro zadání přihlašovacích údajů. Údaj o původně požadované stránce je součástí odeslaného řetězce obsahujícího adresu pro přesměrování uživatele (parametr *RETURNURL*).
3. Na základě přijatého řetězce pak prohlížeč odešle požadavek na zobrazení přihlašovací stránky. Součástí tohoto řetězce je stále údaj o původní požadované stránce.
4. Ze serveru je odeslána stránka s formulářem pro zadání přihlašovacích údajů.
5. Po zadání těchto údajů uživatelem je spolu s parametrem *RETURNURL* stránka odeslána na server.
6. Webová aplikace provede ověření přihlašovacích údajů s položkami v datovém úložišti a v případě úspěšného ověření vytvoří autentizační soubor *cookie*. V opačném případě je uživatel přesměrován zpět na stránku pro přihlášení.
7. Identita uživatele je úspěšně ověřena, server zajistí přesměrování na původní požadovanou stránku podle adresy uložené v parametru *RETURNURL* a poskytne klientské aplikaci soubor *cookie* pro autentizaci při dalším požadavku.
8. Prohlížeč odešle požadavek na původní zabezpečenou stránku stejným způsobem jako v prvním kroku, tentokrát však spolu s údaji autentizačního souboru c*ookie*.
9. Webová aplikace zpracuje požadavek obdobně jako ve druhém kroku, avšak nyní je úspěšně nalezen autentizační soubor a identita uživatele je tím ověřena.
10. Uživateli je zpřístupněna a zobrazena původně vyžadovaná stránka *Default.aspx.*

V případě, že pro přihlášení uživatele použijeme již existující komponentu *Login*, která je součástí *ASP.NET*, pak není potřeba implementovat kroky 7 až 10, jelikož tato komponenta již implementaci dokončení procesu autentizace obsahuje. Podrobnější informace k zabezpečení technologie ASP.NET jsou k vyhledání v publikacích [12] a [13].

3.2.2 Zabezpečení aplikace pro řízení inteligentního domu

Konfigurační soubor *web.*config, v němž má webová aplikace uloženo nastavení jednotlivých prvků, byl upraven podle výše zmíněných možností technologie *ASP.NET.*

```
<authorization>
    <deny users="?" />
</authorization>
<authentication mode="Forms">
    <forms
     name=".ITHouseCookie"
     loginUrl="login.aspx"
     protection="All"
     timeout="30"
     path="/">
```

```
        </forms>
    </authentication>
    ...
```

V sekci <*authorization*> je nastaveno zamezení přístupu anonymní identitě v rámci autorizace. Autentizace je pak prováděna prostřednictvím formuláře na stránce *login.aspx*. Soubor *cookie* není nastaven jako perzistentní, časový interval pro vypršení platnosti autentizace je nastaven na 30 minut.

3.2.2.1 Formulář pro zadání přihlašovacích údajů

Prvním krokem při implementaci zabezpečení aplikace bylo vytvoření přihlašovací stránky *login.aspx*. Zdrojový kód stránky je následující, pro jednoduchost jsou vynechány nepodstatné části kódu.

```
<body>
  <form id="form1" runat="server">
  <asp:Label ID="Label1" runat="server" Text="Jméno:" Font-Bold="True"></asp:Label>
  <asp:TextBox ID="TextBox1" runat="server"></asp:TextBox>
  <asp:RequiredFieldValidator ID="RequiredFieldValidator1" runat="server"
    ControlToValidate="TextBox1" ErrorMessage="Chybí
jméno."></asp:RequiredFieldValidator>
  <asp:Label ID="Label2" runat="server" Text="Heslo:" Font-Bold="True"></asp:Label>
  <asp:TextBox ID="TextBox2" runat="server" TextMode="Password"></asp:TextBox>
  <asp:RequiredFieldValidator ID="RequiredFieldValidator2" runat="server"
    ControlToValidate="TextBox2" ErrorMessage="Chybí
heslo."></asp:RequiredFieldValidator>
  <p>
    <asp:Button ID="Button1" runat="server" Text="Button" onclick="Button1_Click" />
  </p>
  <asp:Label ID="Label3" runat="server" ForeColor="Red"></asp:Label>
  </form>
</body>
</html>
```

Tato stránka obsahuje dvě textová pole pro zadání uživatelského jména a hesla, tlačítko pro odeslání informací a validátory pro správné podoby zadaných údajů. Pro informaci o neúspěšné autentizaci uživatele je přidán popisek se zprávou o chybě.

3.2.2.2 Využití formátu *XML* pro uložení informací o uživatelských účtech

Pro uložení přihlašovacích údajů jednotlivých uživatelů byl zvolen soubor ve formátu *XML* obsahující uživatelské jméno a heslo. Hesla pro přihlášení k jednotlivým účtům jsou ukládána již v zašifrované podobě, aby bylo zamezeno zneužití.

Ponecháme-li u souboru koncovku "*.xml*", mohlo by dojít k nežádoucímu stažení souboru a následně k potenciálnímu zneužití údajů. Přestože jsou hesla již zašifrována, je vhodné jako další bezpečnostní krok změnit koncovku souboru na "*.config*", čímž zajistíme znepřístupnění souboru ze sítě internet.

3.2.2.3 Aplikační logika pro ověření identity uživatele

Po odeslání přihlašovacích údajů je zavolána metoda pro ověření identity uživatele. Tato metoda je obsažena v tzv. *code behind* stránky *login.aspx*, který zajišťuje aplikační logiku. Zdrojový kód je obsažen v souboru *login.aspx.cs*.

Ověření identity uživatele probíhá následujícím způsobem. Po stisknutí tlačítka je vytvořen objekt typu *DataSet*, který slouží jako obraz databáze či v tomto případě *XML* souboru. Struktura souboru je načtena do tohoto objektu společně s daty, jenž obsahují údaje o uživatelských účtech. Jednotlivé položky jsou rozděleny do tabulky, která je automaticky v objektu *DataSet* vytvořena. První položkou každého záznamu je uživatelské jméno, následuje heslo zašifrované algoritmem *MD5* a posledním pdajem je atribut pro určení přístupových práv uživatele. V tomto případě jsou uživatelské účty rozdělené na skupinu běžných účtů a skupinu s administrátorským přístupem.

Autentizace uživatele probíhá ve dvou fázích. Nejprve je zahájeno prohledávání záznamů s uživatelskými účty. Jelikož každé uživatelské jméno je v souboru uloženo jako jedinečné, při prvním úspěšném nalezení ověřovaného uživatelského jména je záznam uložen do objektu *DataRow*. Tento objekt obsahuje všechny tři údaje uchovávané o uživatelském účtu – jméno, heslo a typ účtu. Heslo zadané uživatelem je následně zašifrováno algoritmem *MD5* a porovnáno s odpovídajícím údajem v objektu *DataRow*. Je-li zadané heslo shodné s uloženým, autentizace uživatele je dokončena a dojde k přesměrování na původně požadovanou stránku. Zároveň dojde k ověření, zda uživatel je přihlášen k účtu běžného typu či účtu s administrátorským přístupem. Jedná-li se o účet běžného typu, dojde k zamezení přístupu k položce pro správu uživatelů. Tuto možnost mají pouze uživatelé s administrátorským účtem.

3.3 Webová aplikace

Pro obousměrnou komunikaci uživatele se systémem řízení inteligentního domu byla vytvořena webová aplikace, která je dostupná prostřednictvím webového rozhraní. Na počítači s korektně nastaveným přístupem do sítě, ve které je připojen systém řízení inteligentního domu, lze spustit webového klienta pro spojení s webovým serverem. Tento klient pak zprostředkuje uživateli stránky pro prezentaci a nastavení konfigurace systému.

Webová aplikace systému řízení inteligentního domu je navržena tak, aby byla schopna prezentovat dostupná nastavení a všechny provozní režimy systému a umožňovala nakonfigurovat zařízení do uživatelem požadovaných stavů.

Součástí hlavní stránky webové aplikace je tlačítko pro bezpečné odhlášení uživatele. Obslužná metoda tlačítka pak při požadavku na odhlášení aktuálního uživatele provede automaticky smazání autentizačního souboru *cookie*, čímž okamžitě zamezí zneužití uživatelského účtu třetí osobou. V případě, že by se uživatel po ukončení práce s aplikací neodhlásil, dojde ke smazání autentizačního souboru až po uplynutí časového intervalu. Tím je však uživatelský účet vystaven určitému bezpečnostnímu riziku.

3.3.1 Správa uživatelů

Pro správu registrovaných uživatelských účtů je určena webová stránka s tabulkou, jejíž zdrojem dat je *XML* soubor s údaji o uživatelích. Tato stránka je zpřístupněna pouze tehdy, má-li identita uživatele přihlášeného do systému administrátorská přístupová práva. Pro správu uživatelů jsou k dispozici funkce přidání nového uživatele spolu s nastavením administrátorského přístupu, editace a mazání existujících uživatelských účtů.

3.3.2 Ovládání vstupních a výstupních portů serveru

Jednou z nejdůležitějších součástí celého softwarového řešení systému pro řízení inteligentního domu je knihovna umožňující komunikaci prostřednictvím sériových portů počítače s využitím technologie ASP.NET. Tato knihovna je napsána v jazyce Visual Basic .NET a jejím autorem je italský programátor, pan *Corrado Cavalli*. Po domluvě byla s jeho výslovným souhlasem a velmi vstřícným přístupem tato knihovna použita v rámci diplomové práce pro přístup webové aplikace k sériovému portu webového serveru.

3.3.3 Knihovna RS232

Třída *RS232* obsažená v knihovně *RS232.dll* obsahuje všechny metody, které jsou potřebné pro ovládání sériového portu počítače prostřednictvím webové aplikace systému pro řízení inteligentního domu.

Vytvořením instance třídy je zajištěn přístup k metodám pro nastavení požadovaného sériového portu. Po úspěšné inicializaci je port otevřen a je zahájena komunikace s připojenými zařízeními inteligentního domu. Rozhraní poskytované knihovnou umožňuje nastavení výstupních pinů portu podle požadavků přicházejících z webové aplikace. Jsou-li na sériový port odeslány informace z externích připojených zařízení, pak je nad portem vyvolána událost, která je obsloužena příslušnou metodou a dojde k provedení požadované akce. Touto akcí může být například přímé ovlivnění výstupu sériového portu a odeslání zpravidla upravených dat na akční členy systému spojené s uložením záznamu o provedeném úkonu nebo zobrazení načtených dat ve webovém prohlížeči připojeného uživatele. Podrobnější informace k použité knihovně jsou k vyhledání v publikací [14].

3.4 Připojení částí systému k řídící jednotce z hlediska programového vybavení

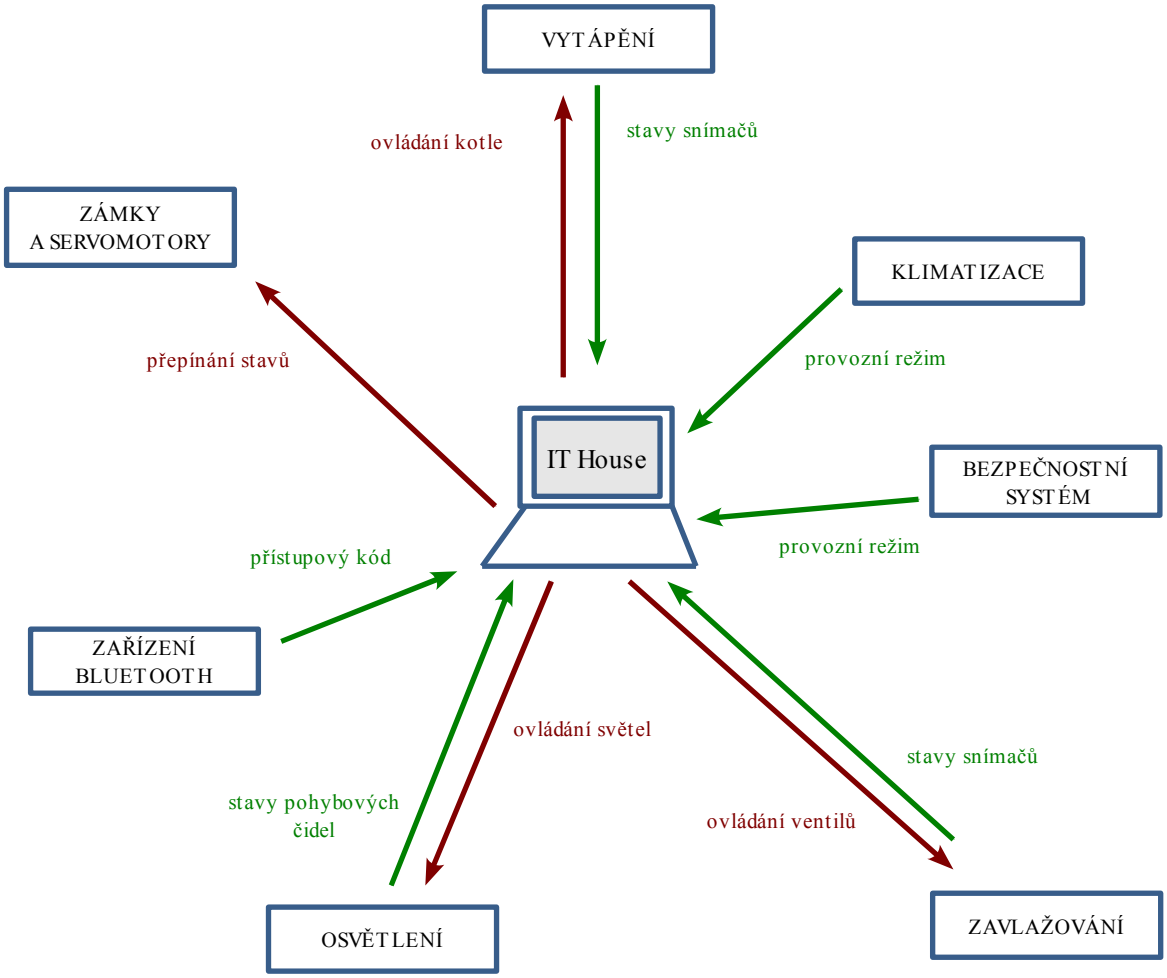
Jednotlivé části systému pro řízení inteligentního domu jsou ovládány prostřednictvím výstupních informací sériového portu. Výstupy jsou navíc ovlivněny vnitřní konfigurací systému, aktuálním požadovým nastavením ze strany uživatele a u některých zařízení také přímo údaji vyhodnocenými vstupními zařízeními sériového portu. Každá část systému má své specifické nastavení a propojení mezi vstupními a výstupními daty.

3.4.1 Návrh systému

Pro návrh systému a znázornění komunikace hlavní řídící jednotky s připojenými systémy byly sestaveny diagramy, které představují jednotlivé interakce mezi řídícím systémem , kterým je vlastní webová aplikace, a daným modulem v podobě připojeného dílčího systému.

Datové toky

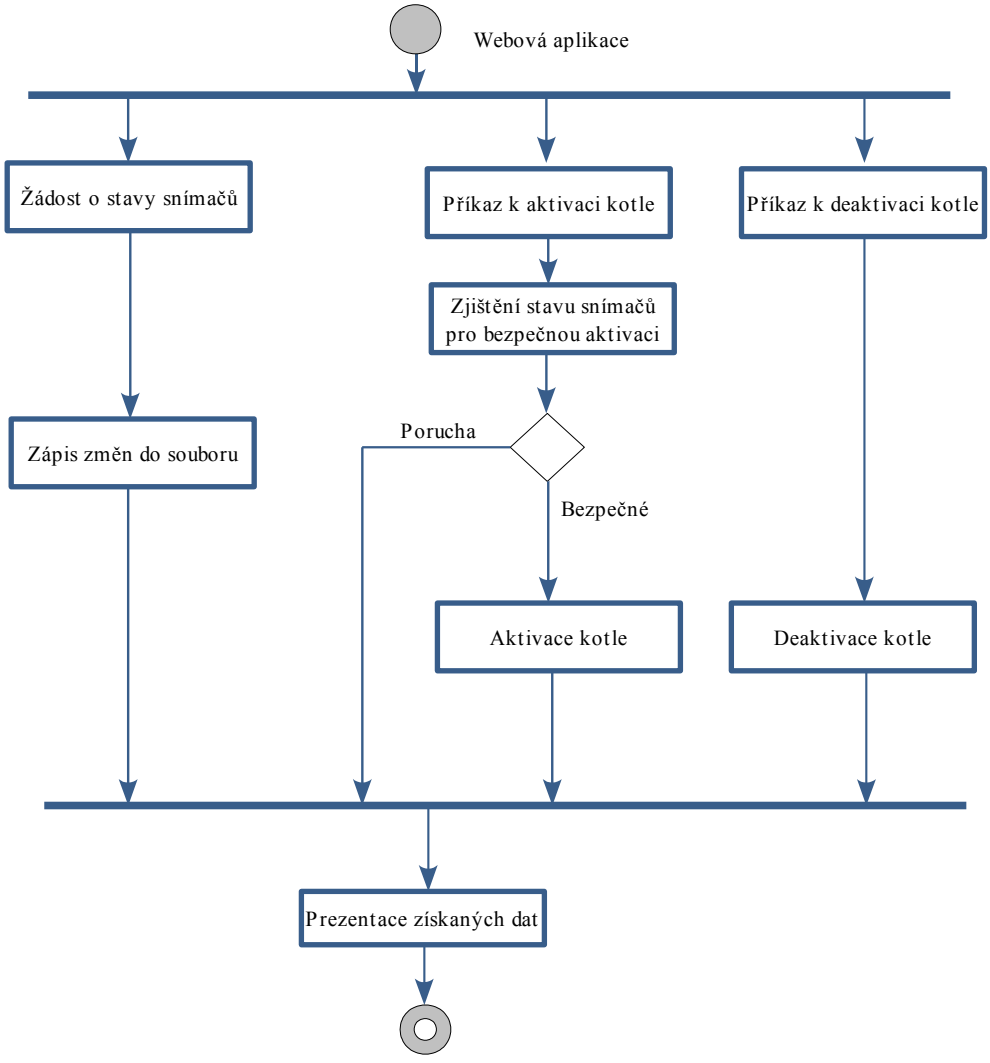
Na obrázku 12 je zakresleno propojení všech modulů s řídícím systémem spolu se zvýrazněním jednotlivých datových toků. Výstupní informace pro ovládání koncových zařízení jsou vyznačeny červenou barvou. Koncovými zařízeními jsou daného systému – v otopném systému se jedná o aktivaci či deaktivaci kotle, u systému osvětlení jsou to vlastní osvětlovací prvky, v zavlažovacím systému jsou ovládány jednotlivé ventily a u modulu pro ovládání zámků a servomotorů jsou koncovými prvky příslušné elektromagnetické kontakty a elektromotory.



Obr.12: Datové toky mezi systémem a připojenými moduly

3.4.1.1 Systém vytápění

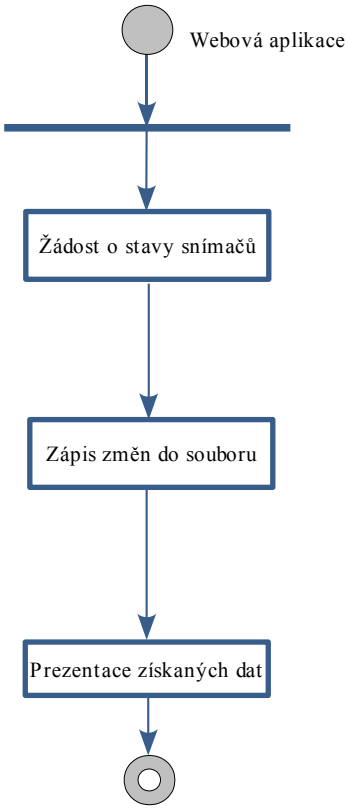
Modul systému vytápění poskytuje řídícímu systému informace o stavech jednotlivých snímačů a je schopen reagovat na podnět řídící jednotky na okamžitou aktivaci či deaktivaci kotle. Komunikace s modulem je znázorněna na obrázku 13. Webová aplikace odesílá periodicky na rozhraní počítače žádost o zjištění stavů snímačů otopného systému. Pokud je zjištěna změna proti informacím získaným v předchozí periodě, pak je proveden zápis aktuálních dat do souboru. Výstupní akcí webové aplikace, která přímo ovlivňuje provozní režim vytápění je příkaz k okamžité deaktivaci či aktivaci kotle. V případě, že je požadována aktivace kotle z vypnutého stavu, je nejprve zkontrolován stav jednotlivých snímačů v otopném systému a teprve v případě, že systém není ve stavu poruchy dojde k aktivaci kotle.



Obr.13: Diagram komunikace s modulem systému vytápění

3.4.1.2 Klimatizace

Systému klimatizace je připojen podobným způsobem jako otopný systém. Nejsou zde však signály pro přímé ovlivnění provozního režimu klimatizace, informace proudí pouze z modulu do řídící jednotky inteligentního domu a slouží výhradně pro monitorování klimatizačního procesu. Na obrázku 14 je popis komunikace mezi modulem a webovou aplikací. Podobně jako u monitorování otopného systému také v tomto případě je periodicky odesílána žádost o výstupní data modulu. V případě změny dat vzhledem k posledním známým údajům jsou informace zapsány do souboru a prezentovány uživateli.



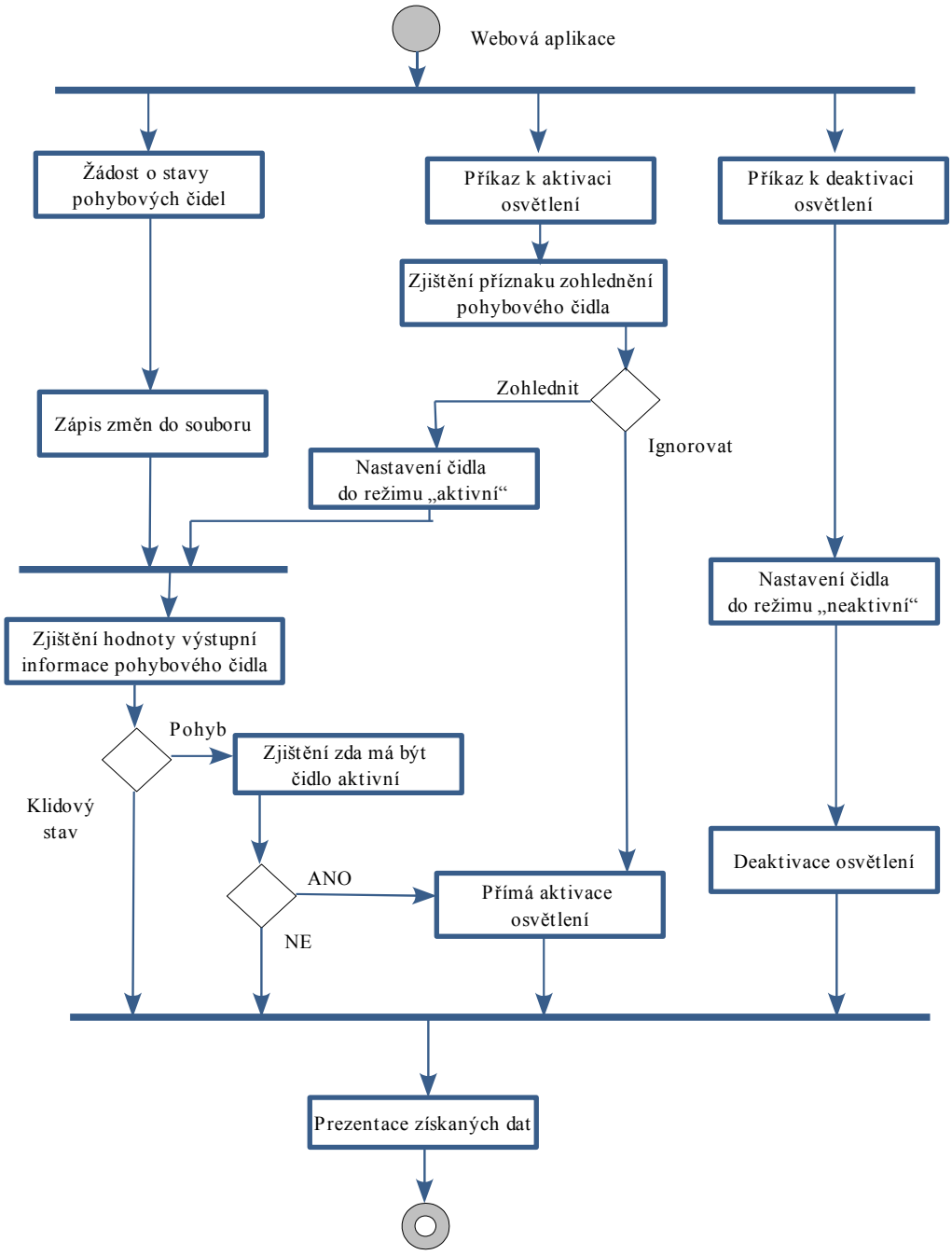
Obr.14: Diagram komunikace s modulem klimatizace

3.4.1.3 Osvětlení

Připojení osvětlovacích prvků budovy k systému řízení inteligentního domu zahrnuje načítání výstupních hodnot pohybových čidel a ovládání osvětlení v závislosti na těchto hodnotách a přednastaveném čase. Diagram znázorňující tuto komunikaci je na obrázku 15.

Aplikace zajišťuje periodické odesílání požadavku na stav připojených pohybových senzorů a v případě změny zapíše novou informaci do souboru. V případě zjištění, že výstupní signál odpovídá detekci pohybu v hlídaném prostoru, dojde k ověření, zda je příslušné čidlo v aktivním či neaktivním režimu. Aktivním režimem je myšlen stav čidla, kdy je aktuální čas události obsažen v intervalu nastaveném pro aktivaci přidruženého osvětlení. V tomto časovém intervalu je čidlo aktivní a umožňuje rozsvícení osvětlení při detekci pohybu. Čidlo přejde do režimu „aktivní“ při vyvolání události pro aktivaci osvětlení, která je spuštěna v přednastavený čas zahájení. Po vyvolání této události dojde k ověření příznaku čidla, zda má být zohledněno při aktivaci osvětlení či nikoliv. Není-li zohlednění čidla aktivováno, dojde k přímému rozsvícení osvětlovacího prvku. V opačném případě je čidlo nastaveno do režimu „aktivní“ a proces pokračuje vyhodnocením detekce pohybu v hlídaném prostoru stejným způsobem jako při periodických požadavcích aplikace.

V přednastaveném čase ukončení režimu osvětlení daného prostoru dojde k vyvolání události pro zajištění vypnutí osvětlovacího prvku. Současně s nastavením přidruženého čidla do režimu „neaktivní“ je pak provedena deaktivace příslušného svítidla. Diagram pro ilustraci výše zmíněných procesů je znázorněn na následujícím obrázku.



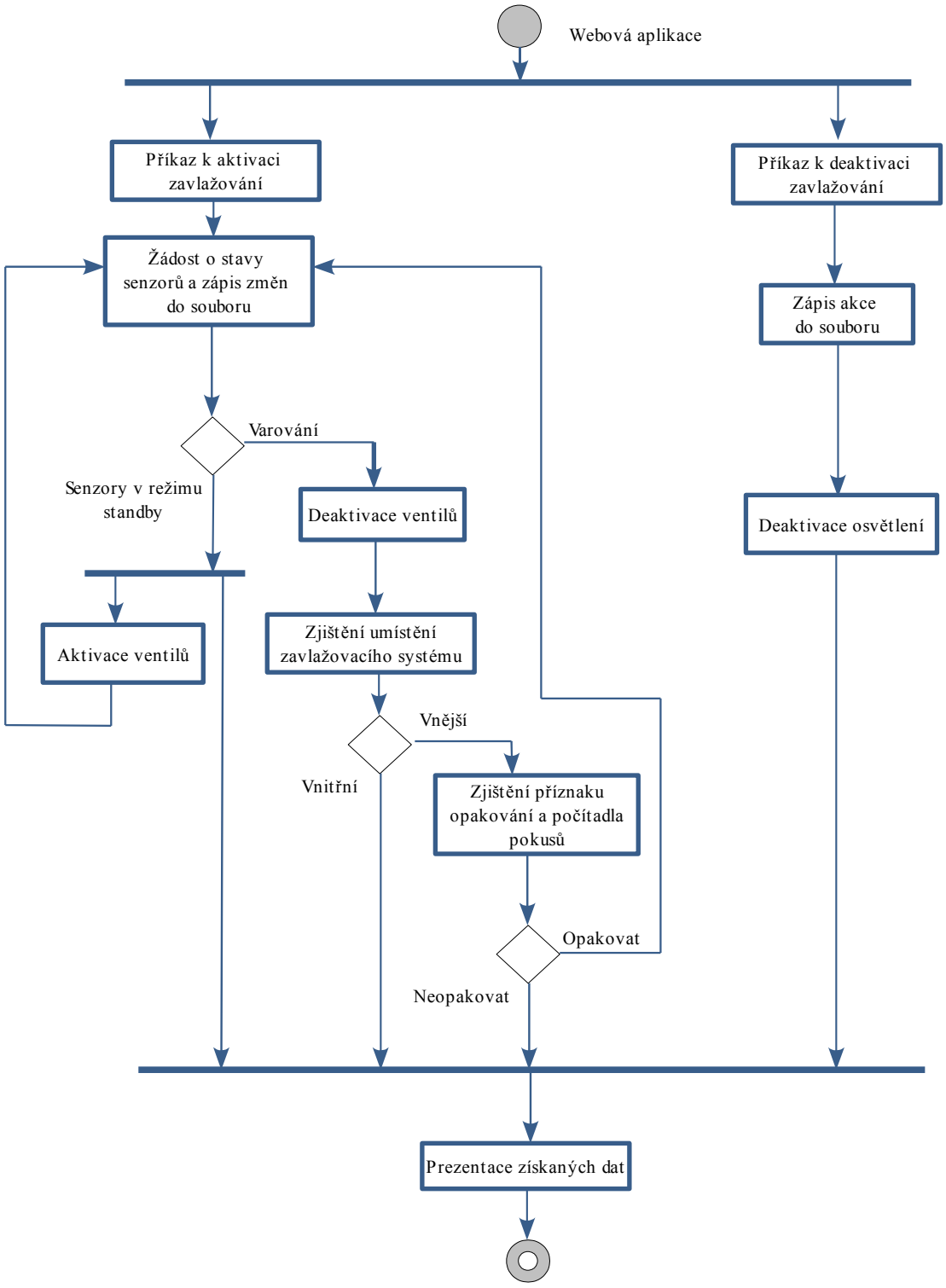
Obr.15: Diagram komunikace s modulem systému osvětlení

3.4.1.4 Zavlažování

Zavlažovací systém připojený k řídící jednotce poskytuje informace o vlhkosti půdy, teplotě vzduchu, intenzitě slunečního záření, pohybu osob v okolí vyústění zavlažovacích prvků a v případě vnitřního systému bezpečnostní detekci přetečení nádoby. Diagram znázorňující jednotlivé kroky při regulaci zavlažovacího systému je na obrázku 16.

V čase zahájení zavlažovacího cyklu, který je nastaven uživatelem, dojde k vyslání příkazu pro aktivaci ventilů. Samotné aktivaci však předchází řada kroků. Nejprve jsou načtena data ze snímačů a případné změny zapsány do souboru. Následuje vyhodnocení stavů senzorů a v případě, že senzory jsou v režimu *standby*, tedy není aktivována žádná z možností varování, dojde k přímé aktivaci přidružených ventilů a k zahájení zavlažovacího cyklu. Dále pak systém pokračuje periodickým načítáním informací ze senzorů a v případě varování dojde k okamžitému vypnutí ventilů. Při přechodu kteréhokoliv senzoru do režimu varování dojde ke zmíněné deaktivaci ventilů a v případě vnitřního zavlažovacího systému k okamžitému ukončení zavlažovacího cyklu spolu s prezentací výsledků v uživatelském rozhraní. Pokud se jedná o venkovní zavlažovací systém, tak v tomto případě nedojde k okamžitému ukončení, ale nejprve se ověří nastavení příznaku pro opakování zavlažovacího cyklu. Pokud je opakování povoleno, tak dojde k opětovné kontrole stavů senzorů a vyhodnocení zahájení zavlažovacího cyklu. Teprve po třech pokusech o obnovení cyklu dojde k ukončení zavlažování a přechodu do neaktivního režimu systému.

Celý zavlažovací proces je přerušen nejen varovnými informacemi senzorů, ale ukončením intervalu zavlažování v přednastaveném čase. V tom případě dojde k vyslání příkazu pro deaktivaci ventilů, prováděná akce se spolu s časovým údajem zapíše do souboru a zavlažovací ventily se vypnou.



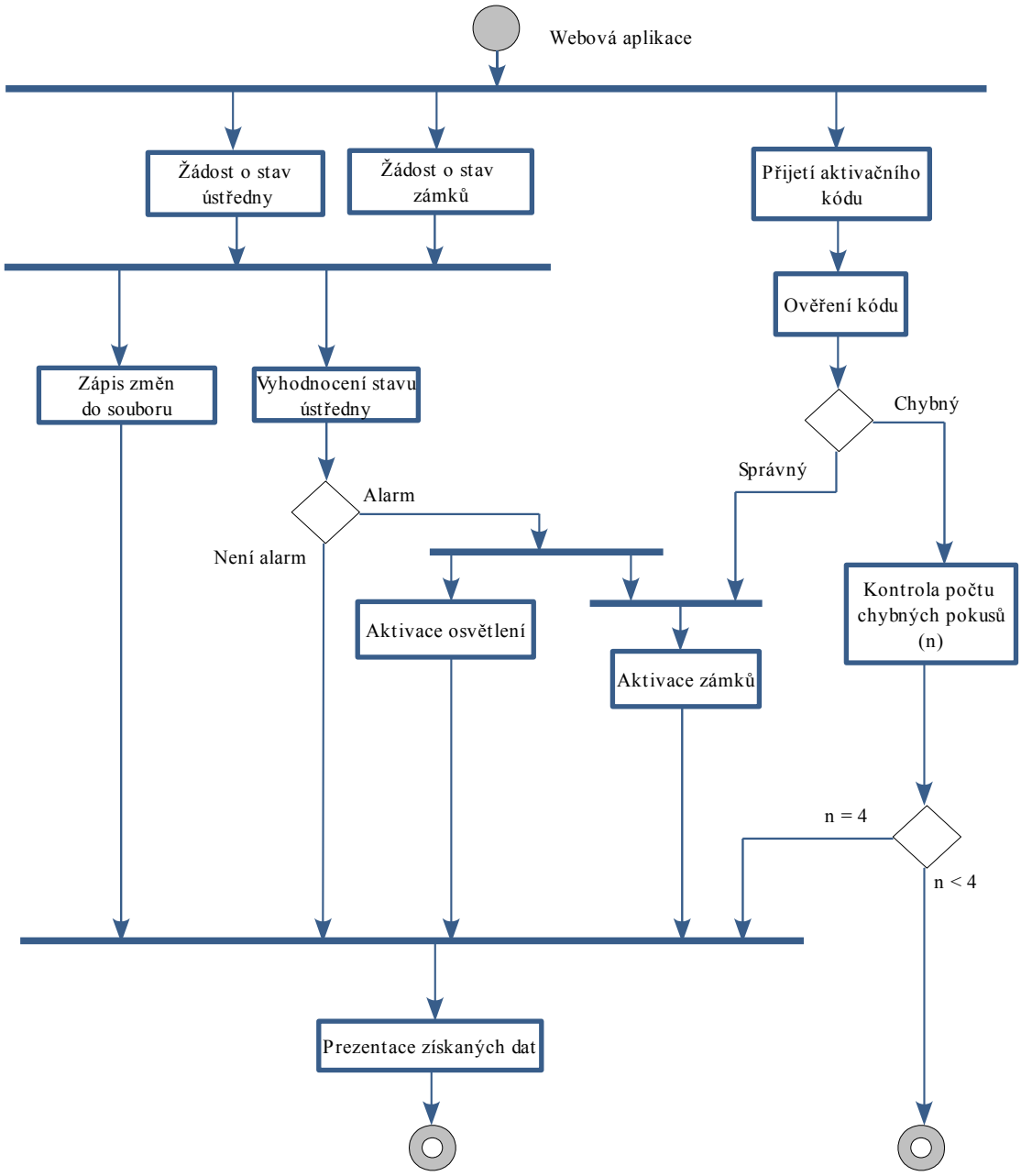
Obr.16: Diagram komunikace s modulem zavlažovacího systému

3.4.1.5 Zabezpečovací systém

Diagram na obrázku 17 popisuje postup při komunikaci s modulem pro zprostředkování informací z bezpečnostní ústředny, modulem pro ovládání zámků a servomotorů a modulem pro bezdrátový příjem aktivačních kódů pro přístup do objektu.

Při komunikaci s modulem bezpečnostního systému je odeslána žádost o stav bezpečnostní ústředny. Stejným způsobem probíhá získání informací o stavu jednotlivých zámků. Načtená data jsou porovnána s posledními uloženými hodnotami a případné změny jsou zapsány do souboru a prezentovány v uživatelském rozhraní aplikace. V případě, že modul bezpečnostního systému hlásí alarm, dojde k okamžité aktivaci přednastavených prvků. Těmi jsou části systému osvělení, elektromagnetické zámky a servomotory přístupových bodů areálu. Tyto prvky jsou v systému přidruženy k příslušnému čidlu pohybu, které je možno v rámci zabezpečení nastavit jako aktivní a tím zajistit okamžitou aktivaci přidruženého osvětlení a zámku.

Druhou částí bezpečnostního systému je ovládání zámků prostřednictvím bezdrátové tecchnologie bluetooth. Po přijetí kódu prostřednictvím připojeného bluetooth modulu aplikace zajistí porovnání kódu s údaji uloženými v šifrovaném souboru. Pokud je kód nalezen, dojde k aktivaci přidružených koncových prvků v podobě zámků či servomotorů. V případě, že je přijatý kód nekorektní, pak aplikace zjistí dosavadní počet chybných pokusů a pokud je překročen přednastavený limit maximálních tří chybných pokusů, dojde k prezentaci této skutečnosti v uživatelském rozhraní. V opačném případě aplikace přijatý kód ignoruje.



Obr.17: Diagram komunikace s modulem zabezpečovacího systému, modulem pro ovládání zámků a modulem pro bezdrátový příjem aktivačního kódu přístupových bodů

3.4.2 Uživatelské rozhraní

Webová aplikace, která plní funkci uživatelského rozhraní, je navržena tak, aby byla ve vývojovém prostředí umožněna poměrně rychlá změna vzhledu jednotlivých komponent. Tato možnost poskytuje přizpůsobení individuálním požadavkům uživatele na vzhled aplikace. V následujících kapitolách je popsána administrátorská část uživatelského rozhraní. U běžného uživatelského účtu bez administrátorského přístupu je zakázáno nastavení a prezentace některých funkcí systému, zejména v části správy uživatelských účtů a nastavení zabezpečovacího systému.

3.4.2.1 Systém vytápění

Věškeré informace jsou periodicky načítány z posuvného registru připojeného k sériovému portu počítače. Bitová mapa načtených dat je spolu s časovým údajem události ukládána v podobě jednotlivých záznamů do souboru s názvem *heating.log,* z tohoto souboru je později možné načíst jednotlivé údaje a ilustrovat průběh regulace vytápění budovy spolu s provozními režimy jednotlivých částí systému. Aktuální hodnoty jsou s každou periodou také zobrazovány v jednotlivých informačních polích webové aplikace v části určené pro prezentaci stavu systému vytápění.

Obr.18: Monitorování vytápění budovy

Webové stránky pro ovládání kotle a monitorování provozních režimů soustavy jsou znázorněny na obrázku 18. Ke každému snímanému prvku lze přidat vlastní popis pro bližší specifikaci. Havarijní stavy pojistek jsou zvýrazněny, aby došlo k okamžitému upozornění obsluhy. Uložením změn v jednotlivých polích dojde k přepsání konfigurační části přidruženého souboru a k uložení uživatelských popisů. Aplikace umožňuje ovládání kotle v podobě okamžité aktivace či deaktivace. Vlastní logika režimu kotle při havarijním stavu je řízena nezávislou vnitřní řídící jednotkou, která zajistí okamžitou deaktivaci v případě poruchy. Signály vlastní řídící jednotky kotle mají rozhodující slovo při reaktivaci vyhřívání, nelze je prostřednictvím uživatelského rozhraní systému inteligentního domu obejít. Závada musí být odstraněna a teprve pak lze vytápění obnovit. Deaktivace kotle je dostupná v jakémkoliv režimu a slouží především k rychlému předcházení nečekaných poruch, které nejsou monitorovány vlastním systémem kotle, příkladem může být prasklé potrubí či požár.

Vyhodnocení naměřených dat a provozních režimů systému vytápění může sloužit k názorné prezentaci režimů systému a efektivnímu nastavení jednotlivých prvků.

3.4.2.2 Klimatizace

Při monitorování systému klimatizace je každá změna vstupních hodnot zaznamenána spolu s časovým údajem události do přidruženého souboru *air_condition.log*, odkud je umožněno podobně jako u systému vytápění načíst jednotlivé záznamy pro ilustrativní zobrazení provozu klimatizace. Tato funkce slouží zejména pro efektivní nastavení systému a využití energie, nejsou dostupné žádné ovládací či regulační prvky pro nastavení klimatizace prostřednictvím uživatelského rozhraní inteligentního domu. Stránka pro monitorování klimatizace je na obrázku 19.

K dispozici je indikace výstupního požadavku bezdrátového termostatu a monitorování pracovního režimu klimatizační jednotky. K jednotlivým položkám je možnost nadefinování podrobnějšího popisu. Při uložení změn dojde k zápisu poznámek do konfigurační části přidruženého souboru.

Obr.19: Monitorování systému klimatizace

3.4.2.3 Osvětlení

Webová aplikace poskytující informace o systému osvětlení budovy má za úkol periodicky načítat data z připojených zařízení a provádět přednastavené obslužné akce. Každá změna vstupních a výstupních informací je uložena spolu s časovým údajem a identifikátorem události do souboru *lights.log*. Odtud je možné načíst poslední známou konfiguraci systému při jeho spuštění a obnovení činnosti podle požadovaného nastavení. Dalším využitím je, podobně jako u ostatních částí systému, možnost vyhodnocení průběhu režimů systému osvětlení v závislosti na čase a případné efektivnější nastavení pro budoucí provoz.

Uživatelské rozhraní této části systému obsahuje seznam všech osvětlovacích prvků a pohybových čidel, u nichž je provedeno připojení k řídící jednotce inteligentního domu. Jednotlivé části umožňují uživatelské pojmenování prvku a nastavení periodického spínání v režimu 24 hodin.Při změně aktuálního stavu osvětlení například vlivem pohybu osob dojde k prezentaci tohoto stavu u příslušného prvku. U každého osvětlovacího koncového zařízení je přidružen snímač pohybu, který lze nastavit do režimu hlídání zaškrtnutím příslušného ovládacího prvku aplikace.

Stránka pro ovládání osvětlení objektu je zobrazena na následujícím obrázku.

Obr.20: Stránka pro ovládání osvětlení

3.4.2.4 Zavlažování

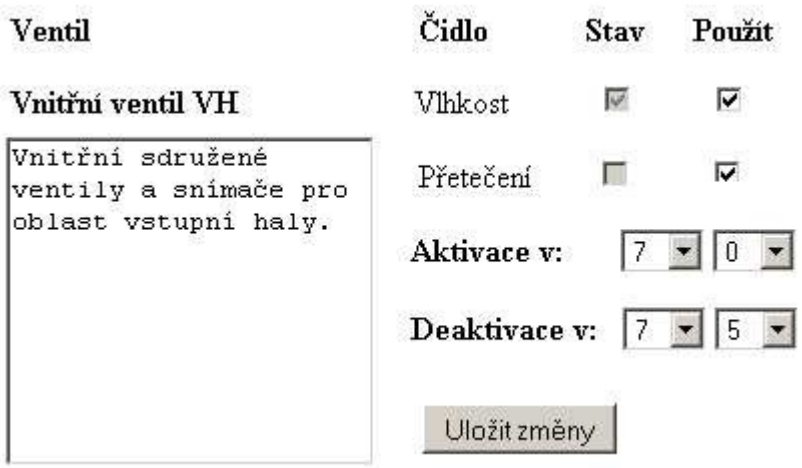
Vstupní a výstupní informace zavlažovacího systému jsou podobně jako v předchozích případech ukládány do souboru *plants.log*. Tento soubor slouží k uchování veškerých informací o komunikaci počítače se zavlažovacím systémem, navíc obsahuje konfiguraci zavlažovacích programů a poslední funkční nastavení systému v případě nekorektního ukončení aplikace či vzniku neočekávané chyby.

Prostřednictvím webové stránky lze ke každému koncovému zařízení v podobě samostatných či sdružených ventilů nastavit provozní režim v závislosti na signálech z příslušných snímačů. Aktuální stavy jednotlivých čidel jsou zobrazeny ve sloupci *Stav*, v dalším sloupci je pak volba, zda má být signál snímače zohledněn při aktivaci zavlažovacího cyklu. Mezi jednotlivými volbami je vztah logického součinu, to znamená, že pro úspěšnou aktivaci procesu musí být zaškrtnuté snímače v režimu *standby* a nesmí na nich dojít k vyvolání příslušného varovného stavu. V případě, že z nějakého důvodu nedojde v zadaný čas k aktivaci koncového prvku, může dojít k opětovnému pokusu po jedné minutě od neúspěšné aktivace. Počet maximálních pokusů po nastavení této volby je pevně stanoven na tři. Při neúspěšném posledním pokusu je systémem zobrazeno varování a k dalšímu pokusu o aktivaci dojde až po běžném 24 hodinovém cyklu.

Obr.21: Zavlažování – exteriéry

Venkovní zavlažovací systém, jenž je zobrazen na obrázku 21, je v některých případech nestandartně vybaven čidlem přetečení, které má za úkol hlídat hladinu kapaliny zejména u rostlin v nádobách umístěných na povrchu, který není schopen pohltit nadbytečné množství vody. Příkladem může být vydlážděné nádvoří nebo dřevěná terasa.

Zavlažovací systém v interiéru budovy se liší od předchozí verze zejména sdruženými ventily pro větší počet zavlažovaných míst a absencí senzoru intenzity slunečního svitu, teploty vzduchu a pohybu osob, které by v tomto případě postrádaly smysl. Nezbytným prvkem je však v tomto případě bezpečnostní snímač přetečení, který má za úkol okamžité uzavření ventilu a upozornění na havarijní stav. Na rozdíl od venkovního zavlažovacího systému není v tomto případě možnost nastavení opakovaného pokusu o aktivaci procesu. Vzhledem k použitým snímačům by takové nastavení bylo zbytečné a v některých případech i nežádoucí (např. opětovný pokus po přetečení nádoby). Nastavení vnitřního zavlažovacího systému je znázorněno na následujícím obrázku.



Obr.22: Zavlažování - interiér

3.4.2.5 Zabezpečovací systém

Připojení ústředny zabezpečovacího zařízení prostřednictvím modulu JA-68 umožňuje monitorování provozních režimů systému a prezentaci zjištěných dat v uživatelském rozhraní webové aplikace. Webová stránka pro zobrazení aktuálního stavu ústředny znázorněná na obrázku 23 umožňuje nastavení reakce osvětlení objektu při narušení bezpečnostních okruhů. Jednotlivými volbami je možné nastavit snímače pohybu a jejich přidružené osvětlovací prvky tak, aby v případě narušení došlo k okamžité aktivaci přednastavených zámků a osvětlení narušené oblasti či celého areálu budovy pro efektivnější vyhledání příčiny narušení.

Ovládání zámků prostřednictvím BT technologie

Do šifrovaného souboru *securityBT.log* jsou uloženy bezpečnostní kódy přidružené k jednotlivým zámkům pro přístup do budovy. Dojde-li k aktivaci virtuálního portu bluetooth modulu vlivem příchozí zprávy z předem spárovaného zařízení, pak je vyvolána příslušná akce, která spočívá v načtení příchozího kódu, prohledání souboru a nalezení přidruženého zařízení k přijatému kódu, dále pak kontroly přístupových práv odesílatele a zjištění režimu bezpečnostního systému. V závislosti na aktuální konfiguraci je aktivován či deaktivován přidružený akční člen.

Součástí stránky pro monitorování a nastavení části bezpečnostního systému je možnost prezentace a změny aktivačních hesel k jednotlivým přístupovým bodům budovy. Změny jsou ukládány do souboru *securityBT.log*. Nastavení těchto prvků je umožněno pouze uživateli s administrátorským přístupem.

Bezpečnostní systém

Bezpečnostní ústředna - stav : *armed* Uložit změny

Pohybová čidla

Kód	Popis	Aktivní
ON1	venkovní-nádvoří vpravo	☐
ON2	venkovní-nádvoří vlevo	☐
OV1	venkovní-hlavní vchod	☑
IG1	vnitřní-garáž 1	☑
IG2	vnitřní-garáž 2	☑
IZ1	vnitřní-zadní vchod	☑
OZ1	venkovní-zadní vchod	☑

Přístupové body

Kód	Popis	Heslo
HV	hlavní vchod	hv552
ZV	zadní-služební vchod	zv559
HB	hlavní příjezdová brána	hb562
ZB	zadní příjezdová brána	zb569
GB1	brána příjezdu ke garážím	gb162
P2	parkoviště-závora 2	pz269
GV	hlavní garáž-závora vjezdu	gv252

Obr.23: Stránky bezpečnostního systému a ovládání zámků

V případě požadavku o aktivaci či deaktivaci zámku u přístupového bodu je přijata informace z modulu bluetooth. Příchozí data z bezdrátového zařízení jsou zaznamenána do souboru *security.log* v podobě časového údaje a identifikačního čísla požadovaného zařízení, se kterým má být manipulováno. Příchozí kód není nikam ukládán, aby nemohlo dojít k jeho nežádoucímu zneužití nepovolanou osobou.

Program pro odeslání přístupového kódu

Ovládání zařízení přidružených k bezpečnostnímu kódu je realizováno prostřednictvím mobilního telefonu podporujícího technologie *bluetooth* a *Java Mobile Information Device Profile (MIDP)* verze *2.0.* Pro tyto potřeby byla vytvořena jednoduchá aplikace v jazyce *Java*, která zajistí bezdrátovou komunikaci mezi mobilním telefonem a *bluetooth* modulem připojeným prostřednictvím USB portu k řídícímu počítači systému.

Prvním krokem při realizaci funkce bezdrátového ovládání bezpečnostních zařízení objektu je registrace konkrétního mobilního telefonu do systému Prostřednictvím obslužného software uskuteční pověřená osoba spárování s *bluetooth* modulem a předá uživateli přístupová hesla k jednotlivým prvkům zabezpečení. Systém je navržen tak, že každý bezpečnostní prvek (zámek dveří, zařízení pro ovládání závory či brány apod.) má přidělen vlastní bezpečnostní kód. Odesláním tohoto kódu v blízkosti zařízení dojde k přechodu režimu zařízení z aktuálního na opačný.

Ověřování hesla a asociaci s příslušným bezpečnostním prvkem zajišťuje hlavní aplikace systému, která naslouchá na přiděleném sériovém portu *bluetooth* modulu a v případě přijetí kódu od autorizovaného (spárovaného) mobilního telefonu zajistí přednastavené akce.

Midlet

Po spuštění aplikace *Remote Security Lock* v mobilním telefonu dojde k vyhledání zařízení dostupných prostřednictvím bluetooth rozhraní. Uživatelské rozhraní umožní výběr příslušného zařízení pro příjem bezpečnostního kódu a po zadání hesla odešle data na modul připojený k počítači. Zde je kód načten obslužnou aplikací prostřednictvím virtuálního sériového portu a dále zpracován. Následuje vyhodnocení požadované akce a v případě úspěšného ověření kódu dojde k aktivaci či deaktivaci příslušného zařízení. Program v jazyce Java pro mobilní zařízení byl vyzkoušen na mobilním telefonu Samsung E250, který splňuje minimální požadavky pro provoz aplikace a odeslání hesla na bluetooth přijímač propojený s USB portem počítače. Při vytváření aplikace bylo využito informací v publikaci [15].

4 Závěr

V této práci byl navržen komplexní systém řízení inteligentního domu. V případě, že dojde k přizpůsobení k individuálním požadavkům uživatelů, vznikne systém s vysokou mírou variability a univerzálního využití. Uplatnění může nalézt nejen ve velkých komplexech budov pro komerční využití, ale také v běžných domácnostech, ať už se jedná o rodinné domy či bytové zástavby. Jelikož byl kladen důraz na minimální pořizovací nároky, ať už finanční či v podobě zásahu do stávajících instalací, nízkou spotřebu energií, náročnost obsluhy a v neposlední řadě nízké provozní náklady, mohlo by dojít k velkému rozšíření takového systému a tím zejména ke zlepšení ekologické situace naší planety. Tento záměr je pro mě hlavním cílem při realizaci projektu inteligentního domu.

5 Literatura

[1] Oficiální stránky společnosti ASUS – http://www.asus.cz

[2] HW server s.r.o. - http://www.hw.cz

[3] Oficiální stránky společnosti DIGITUS – http://www.digitus.info

[4] ComDis s.r.o. - http://www.i-tec.cz

[5] Oficiální stránky společnosti ECOM s.r.o. – http://www.ecom.cz

[6] Veřejné fórum – http://forum.mcontrollers.com/

[7] FCC Public s.r.o. – http://www.odbornecasopisy.cz

[8] ELEKTROBOCK CZ s.r.o. – http://www.elektrobock.cz

[9] JABLOTRON ALARMS a.s. – http://www.jablotron.cz

[10] The Apache Software Foundation – http://www.apache.org

[11] SourceForge.net – http://sourceforge.net

[12] Oficiální stránky časopisu Živě.cz – http://www.zive.cz

[13] Microsoft Corporation – http://msdn.microsoft.com/en-us/library/aa480476.aspx

[14] Codeworks S.a.s, Corrado Cavalli - http://www.codeworks.it/net/VBNetRs232.htm

[15] Zoner software a.s – http://www.interval.cz